COUNCIL

TUESDAY, 15TH MAY 2018, 6.30 PM
COUNCIL CHAMBER, TOWN HALL, CHORLEY

AGENDA

APOLOGIES

1 **MINUTES OF MEETING TUESDAY, 10 APRIL 2018 OF COUNCIL** (Pages 5 - 10)

2 **DECLARATIONS OF ANY INTERESTS**

Members are reminded of their responsibility to declare any pecuniary interest in respect of matters contained in this agenda.

If you have a pecuniary interest you must withdraw from the meeting. Normally you should leave the room before the business starts to be discussed. You do, however, have the same right to speak as a member of the public and may remain in the room to enable you to exercise that right and then leave immediately. In either case you must not seek to improperly influence a decision on the matter.

3 **RETURNING OFFICER'S REPORT**

The Chief Executive as Returning Officer will report that the following persons were duly elected as councillors for the wards stated at the Borough elections on 3 May 2018:

Ward	Councillor
Adlington and Anderton	Graham Dunn
Astley and Buckshaw	Matthew Lynch
Chisnall	Alan Whittaker
Chorley East	Hasina Khan
Chorley North East	Alistair Morwood
Chorley North West	Ralph Snape
Chorley South East	Beverley Murray
Chorley South West	Roy Lees
Clayton-Le-Woods and Whittle-Le-Woods	Eric Bell
Clayton-Le-Woods North	Yvonne Hargreaves
Clayton-Le-Woods West and Cuerden	Neville Whitham
Coppull	Steve Holgate
Eccleston and Mawdesley	Keith Iddon
Euxton North	Thomas Gray
Euxton South	Gillian Sharples
Pennine	Gordon France
Wheelton and Withnell	Margaret France

Meeting contact Ruth Rimmington on 01257 515118 or email ruth.rimmington@chorley.gov.uk

4 **ELECTION OF THE MAYOR FOR THE COUNCIL YEAR 2018/19**

To formally elect the Mayor of the Borough for 2018/19.

5 **ELECTION OF THE DEPUTY MAYOR FOR THE COUNCIL YEAR 2018/19**

To formally elect the Deputy Mayor of the Borough for 2018/19.

THERE WILL BE A SHORT ADJOURNMENT WHILST THE MAYORAL PARTY EXCHANGE ROBES AND BADGES OF OFFICE

6 **VOTE OF THANKS TO THE RETIRING MAYOR**

The Retiring Mayor will receive a vote of thanks for his year in office.

7 **EXECUTIVE CABINET APPOINTMENTS FOR 2018/19**

To receive a report of the Executive Leader (to follow).

8 **APPOINTMENTS TO COMMITTEES, PANELS AND WORKING GROUPS FOR 2018/19**

To approve the appointment of Members of the Council to Committees, Working Groups, etc and to note shadow appointments for 2018/19 (to follow).

9 **APPOINTMENTS TO OUTSIDE BODIES FOR 2018/19**

To appoint Members of the Council to represent the Authority on outside bodies in 2018/19 (to follow).

10 **COUNCIL MEETINGS 2018/19**

To note the programme of Council Meetings for 2018/19:

- Tuesday, 24 July 2018 at 6.30pm
- Tuesday, 18 September 2018 at 6.30pm
- Tuesday, 20 November 2018 at 6.30pm
- Tuesday, 22 January 2019 at 6.30pm
- Tuesday, 26 February 2019 at 6.30pm
- Tuesday, 9 April 2019 at 6.30pm
- Tuesday, 14 May 2019 at 6.30pm

11 **GENERAL DATA PROTECTION REGULATIONS** (Pages 11 - 92)

To consider the report of the Director (Policy and Governance).

12 **LCC TRANSFORMATION FUND - ADDITIONAL BUDGET REQUEST** (Pages 93 - 100)

To consider the report of the Director (Policy and Governance).

13 **EXCLUSION OF THE PUBLIC AND PRESS**

To consider the exclusion of the press and public for the following items of business on the ground that it involves the likely disclosure of exempt information as defined in Paragraph 3 of Part 1 of Schedule 12A to the Local Government Act.

By Virtue of Paragraph 3: Information relating to the financial or business affairs of any particular person (including the authority holding that information)
Condition:
Information is not exempt if it is required to be registered under-
The Companies Act 1985
The Friendly Societies Act 1974
The Friendly Societies Act 1992
The Industrial and Provident Societies Acts 1965 to 1978
The Building Societies Act 1986 (recorded in the public file of any building society, within the meaning of the Act)
The Charities Act 1993
Information is exempt to the extent that, in all the circumstances of the case, the public interest in maintaining the exemption outweighs the public interest in disclosing the information.

Information is not exempt if it relates to proposed development for which the local planning authority may grant itself planning permission pursuant to Regulation 3 of the Town & Country Planning General Regulations 1992(a).

14 **PROPERTIES FOR THE SYRIAN REFUGEE PROGRAMME** (To Follow)

To consider the report of the Director (Early Intervention and Support) (to follow).

15 **ANY URGENT BUSINESS PREVIOUSLY AGREED WITH THE MAYOR**

GARY HALL
CHIEF EXECUTIVE

Electronic agendas sent to Members of the Council.

If you need this information in a different format, such as larger print or translation, please get in touch on 515151 or chorley.gov.uk

To view the procedure for public questions/ speaking click here https://democracy.chorley.gov.uk/documents/s67429/Appendix%203%20Standing%20Orders%20Aug%2016.pdf and scroll to page 46

This page is intentionally left blank

Chorley Council

MINUTES OF **COUNCIL**

MEETING DATE **Tuesday, 10 April 2018**

MEMBERS PRESENT: Councillor Mark Perks (Mayor), Councillor Margaret Lees (Deputy Mayor) and Councillors Aaron Beaver, Eric Bell, Martin Boardman, Alistair Bradley, Charlie Bromilow, Terry Brown, Paul Clark, Jean Cronshaw, Alan Cullens, John Dalton, Christopher France, Gordon France, Margaret France, Jane Fitzsimons, Anthony Gee, Danny Gee, Tom Gray, Keith Iddon, Mark Jarnell, Hasina Khan, Zara Khan, Paul Leadbetter, Roy Lees, Sheila Long, Adrian Lowe, Marion Lowe, Matthew Lynch, June Molyneaux, Greg Morgan, Alistair Morwood, Mick Muncaster, Steve Murfitt, Beverley Murray, Debra Platt, Joyce Snape, Kim Snape, Richard Toon, John Walker, Paul Walmsley, Alan Whittaker and Peter Wilson

OFFICERS: Chris Sinnott (Director (Early Intervention and Support)), Asim Khan (Director (Customer and Digital)), Rebecca Huddleston (Director (Policy and Governance)), Chris Moister (Head of Legal, Democratic & HR Services) and Ruth Rimmington (Democratic and Member Services Team Leader)

APOLOGIES: Councillors Henry Caunce, Doreen Dickinson, Graham Dunn and Ralph Snape

17.C.503 Minutes of meeting Tuesday, 27 February 2018 of Council

Decision: That the minutes of the last Council meeting held on 23 January 2018 be approved as a correct record for signature by the Mayor.

17.C.504 Declarations of Any Interests

There were no declarations of interests received.

17.C.505 Mayoral Announcements

The Mayor referred to the forthcoming elections, wishing all Members well in contesting their councillor seats. In particular he referred to Councillors Charlie Bromilow, Mark Jarnell and Richard Toon who were not seeking re-election and wished them well for the future.

Councillors Alistair Bradley and Alan Cullens paid tribute to the work of the retiring Councillors.

17.C.506 Public Questions

There were no public questions for consideration.

17.C.507 Executive Cabinet

Councillor Alistair Bradley, Executive Leader presented a general report of the Executive Cabinet meetings held on 18 January, 15 February and 15 March.

Councillor Alistair Bradley, Executive Leader proposed, Councillor Peter Wilson, Executive Member for Resources, seconded the **DECISION – that the report be noted.**

17.C.508 Revenue and Capital Budget Monitoring 2017/18 Report 3 (end of December 2017)

Councillor Peter Wilson, Executive Member (Resources) presented the report of the Chief Finance Officer which set out the provisional revenue and capital outturn figures for the Council as compared against the budgets and efficiency savings targets set for the financial year 2017/18.

Councillor Peter Wilson, Executive Member for Resources proposed, Councillor Alistair Bradley, Executive Leader seconded the **DECISION – to**

1. **Note the full year forecast position for the 2017/18 revenue budget and capital investment programme.**
2. **Note the forecast position on the Council's reserves.**
3. **Approve the contribution of £60,000 from in-year revenue underspends to the Buildings Maintenance Reserve to finance one-off costs relating to the Council's maintenance of offices and buildings.**
4. **Approve the contribution of £100,000 from in-year revenue underspends to the Change Management Reserve to finance one-off redundancy and pension strain costs arising from transformation and shared service strategies.**
5. **Approve the contribution of £40,000 from in-year revenue underspends to fund the revenue implications of future planning appeals.**
6. **Approve the use of £40,000 from in-year revenue underspends to provide the council with external expertise for the furthering of income generation.**
7. **Approve the contribution of £130,000 from in-year revenue underspends to enable the modernisation of the Council's ICT and Streetscene services.**
8. **Approve the budget changes to the capital programme outlined in paragraph 70.**

17.C.509 Overview and Scrutiny Committee and Task and Finish Groups

Councillor John Walker, Chair of the Overview and Scrutiny Committee presented a general report of the of the Overview and Scrutiny Committee held on 25 January and 22 March, the Overview and Scrutiny Performance Panel held on 8 March and Task Group update.

Councillor John Walker, Chair of the Overview and Scrutiny Committee proposed, Councillor Roy Lees, Vice Chair, seconded the **DECISION – that the report be noted.**

17.C.510 Governance Committee

Councillor Paul Leadbetter, Chair of the Governance Committee presented a general report on the work of the Committee meeting on 24 January and 21 March.

Councillor Paul Leadbetter, Chair of the Governance Committee proposed, Councillor Anthony Gee, Vice Chair, seconded the **DECISION – that the report be noted.**

17.C.511 Electoral Review of Chorley Council - Draft Council Size Submission

Councillor Alistair Bradley Executive Leader, advised that the first meeting of the Electoral Review of Chorley Council Committee took place on 7 March 2018. At that meeting, the committee considered evidence that is to be presented as part of the council's submission to the LGBCE.

The LGBCE will re-draw ward boundaries so that they meet their statutory criteria. The council will have the opportunity to put forward its ideas in two phases of public consultation.

Councillor Alan Cullens, Leader of the Conservative Group, proposed an amendment, that Chorley Council should comprise of 39 councillors and move to all out elections. This would save the council a considerable sum of money. Councillor Martin Boardman, Shadow Executive Member (Resources) seconded the amendment.

The proposal was put to the vote and **LOST**.

Members considered the disadvantages to all out elections, particularly the political instability this could lead to. Having elections by thirds enabled change to be more gradual and for councillors to build experience on each of the committees. This also acted as a buffer for populism.

Members discussed the importance of having enough councillors to discharge the functions of the council, and to hold the Executive to account.

Councillor Alistair Bradley, Executive Leader proposed an amendment to the council size submission document. On page 3 under the 'Proposal' heading there is a brief summary of the approach taken to develop and agree the council size proposal. The Council's submission has been developed by a cross party committee of 9 councillors. A meeting of the Electoral Review of Chorley Council Committee took place on the 7 March 2018, following a review of evidence, a positive discussion and due consideration the committee unanimously agreed that the council size could be reduced from 47 to be 42 members with the frequency of elections continuing by thirds.

Councillor Alistair Bradley, Executive Leader proposed, Councillor Peter Wilson, Executive Member for Resources, seconded the amended substantive motion, the **DECISION**

To approve the amended council submission on the future size and electoral cycle of Chorley Council, as agreed unanimously at the Electoral Review of Chorley Council Committee, that Chorley Council should –

- **comprise of 42 councillors, and**
- **continue to undertake its elections by thirds**

17.C.512 Council Appointments

Agreement was sought to a new outside body appointment for Chorley Football Club Community Trust.

Councillor Alistair Bradley, Executive Leader proposed, Councillor Peter Wilson, Deputy Leader, seconded and it was **RESOLVED - To appoint the Executive Member (Early Intervention and Support) to Chorley Football Club Community Trust.**

17.C.513 Questions Asked under Council Procedure Rule 8 (if any)

There were no questions for consideration under Procedure Rule 8.

17.C.514 To consider the Notices of Motion (if any) given in accordance with Council procedure Rule 10

There were no motions for consideration under Procedure Rule 10.

17.C.515 To consider petitions (if any) presented in accordance with Council procedure Rule 23

There were no petitions presented in accordance with Council procedure Rule 23.

17.C.516 Exclusion of the Public and Press

Councillor Alistair Bradley, Executive Leader proposed, Councillor Peter Wilson, Deputy Leader seconded **the DECISION that the press and public be excluded for the following items of business due to the disclosure of exempt information under Paragraph 3 of Part 1 of Schedule 12A to the Local Government Act.**

17.C.517 Acquisition of Former Hyatt Restaurant, Dole Lane and Proposed Lease to Chorley Little Theatre

Councillor Peter Wilson, Executive Member (Resources) presented the report of the Director of Business, Development and Growth. The report sought approval to purchase the building known as the former Hyatt Restaurant premises on the terms indicated in the report and shown edged red on the attached plan.

The report also sought approval for a new Lease to be granted to the Chorley Little Theatre for the Hyatt Premises to be able to be occupied in connection with their use of the Chorley Little Theatre for studio space, rehearsals and storage.

Councillor Peter Wilson, Executive Member for Resources proposed, Councillor Alistair Bradley, Executive Leader seconded the **DECISION –**

1. **That Council allocate the budget to be used for the purposes of purchasing the freehold of the Hyatt, 1 Dole Lane, Chorley.**
2. **That Council note that on 15 March the Executive Cabinet resolved**
   a. To proceed with the freehold purchase of the Hyatt Premises, 1 Dole Lane, Chorley, PR7 2RL within the time frame so that preparations can be implemented by the Chorley Little Theatre for expansion and rehearsal rooms.
   b. That authority is to be delegated to the Executive Member for Resources to negotiate the terms of the lease with the Chorley Little Theatre in accordance with those provisionally agreed and contained at paragraph 17.
   c. That the Head of Legal, Democratic and HR Services be authorised to complete the documentation for both the purchase of the freehold from the existing vendor and complete the documentation for a Lease on terms to be negotiated in accordance with paragraph 2 to the Chorley Little Theatre.

Mayor Date

This page is intentionally left blank

Report of	Meeting	Date
Director of Policy and Governance	Council	15 May 2018

GENERAL DATA PROTECTION REGULATIONS

PURPOSE OF REPORT

1. To advise members of the steps taken by this Council to implement the General Data Protection Regulations and to seek the adoption of new policies and appointment of a Data Protection Officer to support this.

RECOMMENDATION(S)

2. That Members approve the adoption of the policies contained at Appendix 1.
3. That Members approve the appointment of the Council's Monitoring Officer, the Head of Legal, Democratic and HR Services to the role of Data Protection Officer.

EXECUTIVE SUMMARY OF REPORT

4. The EU General Data Protection Regulations (GDPR) come into force on 25 May 2018. These introduce a new data protection regime to be enforced against any organisation doing business or providing services within the European Economic Area. This includes Local Government.
5. The GDPR are to be implemented nationally through a new Data Protection Act, although this has not yet been passed by Parliament. The compliance steps taken therefore are to implement the GDPR themselves. It is unlikely there will be a significant departure from them as part of the principle of their adoption was to provide consistency across Europe.
6. The GDPR provide new principals to be applied placing new obligations on data holders and new rights are granted to data owners. These are detailed below in the body of the report. There is also a new role created who is responsible for the monitoring of the Data Protection regime in each organisation, the Data Protection Officer.

Confidential report Please bold as appropriate	Yes	**No**

CORPORATE PRIORITIES

7. This report relates to the following Strategic Objectives:

Involving residents in improving their local area and equality of access for all		A strong local economy	
Clean, safe and healthy homes and communities		An ambitious council that does more to meet the needs of residents and the local area	X

BACKGROUND

8. For many years the Council have been required to comply with the Data Protection Act which governed how we were to hold and use data. The focus was always on the

information itself rather than the ownership. This lead to the misuse of data by some organisations for the purposes of direct marketing, with some even having a business model selling lists of personal data. This was often done without the knowledge of the owner of the data the individual concerned. They generally received no payment for the use of their data and also had the perceived (or real) burden of junk mail, nuisance calls and spam email.

9. The GDPR seek to change this. They make it clear that the owner of the data is not the holder of it but the subject of it. They place obligations on all organisations who process data within the European Economic area and provide new rights for individuals to control the processing of their data.
10. Compliance with these obligations and rights is mandatory and failure to comply could lead to a fine of up to 10 mill Euros for personal data breaches or 20 mill Euros for sensitive data breaches. Members are asked to note that the same regime applies to all organisations whatever the turnover (and there are greater fines which could be imposed depending on global turnover figures, these do not apply to this Council).
11. The key to compliance with the GDPR is a strong governance regime with robust policies and processes in place. In part many of these processes are already established due to the Council's compliance with the Data Protection Act, but it is recognised they require some amendment.
12. In addition the Council are obliged to appoint a Data Protection Officer. They should have received appropriate training on the operation of the GDPR and report into the Senior Management Team of the Council. They should have no responsibilities however for setting compliance policies as they will need to assess performance against them but also assess their continued appropriateness and suitability.

Roles and Definitions

13. The GDPR introduce a number of new roles of persons involved in the processing of data and indeed what constitutes data itself. It is important to know what these roles and definitions are to understand the obligations.

Personal Data	Information belonging to an identified or identifiable natural person. The GDPR do not apply to businesses only individuals. If a person can be identified from the information processed then it is Personal Data.
Sensitive Data	Personal Data particularly sensitive to that individual which is not apparent such as race or ethnicity, political persuasion, religious beliefs, trade union membership, health, sexual orientation. Breach of the GDPR in relation to this category of data can lead to a higher level fine.
Data Owner	Is the Natural Person who can be identified from the Personal Data.
Natural Person	Must a living person and not a 'corporate' entity.
Data Processing	Means any manipulation or use of data and includes both the holding and deletion of Personal Data.
Data Controller	Determines and sets the purpose and means of processing of Personal Data. They will be responsible for setting policies and processes for their team that depart from any corporate approach.
Data Processor	Acts to process the Personal Data at the direction of the Data Controller.
Data Protection Officer	Is responsible for the monitoring of the GDPR regime adopted by the Council both in terms of compliance by council officers but also the suitability of the policies and processes adopted.

Rights of Data Owners

14. The GDPR make it clear that the owner of Personal Data is the subject of that data, ie the person who can be identified from it. To ensure that this ownership is made clear the GDPR bestow rights on the data owner, failure to comply with these rights by a data holder is a breach of the regulations.

15. The rights are as follows:-

To be Informed	Data Owners must be notified what Personal Data organisations hold about them and the purpose it is held.
Access	Data Owners have the right to see all their Personal Data held by the organisation
Rectification	Data Owners are entitled to require that any incorrect Personal Data held by an organisation is corrected
Erasure	Data Owners can require that their Personal Data be deleted. Although this is subject to any legal requirements the Council may have. So for example where Personal Data is held concerning an individuals Council Tax liability then they cannot require it be deleted.
Restrict Processing	Data Owners can insist that their Personal Data is no longer processed for a non-statutory purpose, eg they can request they are no longer contacted for marketing or consultative purposes.
Data Portability	Organisations are required to provide data electronically in a way that can be easily read by the Data Owner, ie in exel or adobe or word.
To Object	Data Owners have the right to challenge the processing of their Personal Data
To limit automated decision making and profiling	This is not undertaken by the Council.

Many of these rights were already inferred by the previous legislation and good practice dictated compliance with an individuals wishes. It is an obligation on the Council to ensure that we can comply with the rights.

16. In order to comply with the right to be informed the Council are implementing an Opt In process for non-statutory uses of Personal Data. The Opt In will inform individuals of the ability for their Personal Data to be used for purposes other than those it was supplied for such as Marketing of Council Services, Marketing of Council Events or Consultations and allow them to opt in for that use. If they do not opt in then the data cannot be used for that purpose.

GDPR Principles

17. When processing Personal Data, the GDPR have now fixed a series of Principles by which organisations should act. These are as follows:-

To act legally, transparently and fairly	Personal Data should only be processed where there is a lawful (generally a statutory reason) basis or where specific consent has been given. The Opt In process referred to at paragraph 16 above enables consent to be given. Consent is also given where the Personal Data is volunteered for the purpose of obtaining/requesting a council service. But the consent is for the Personal Data to be used for that Purpose only.
Purpose Limitation	Where Personal Data has been provided for a particular Purpose (council tax benefit, green waste collection, service request) it can only be used for that purpose unless consent is specifically given for it to be used for another Purpose.
Minimisation	Organisations should only request the Personal Data necessary to discharge the Purpose. For example where someone is applying for a green waste collection we would not need their date of birth.
Accuracy	Organisations are obliged to ensure that the data held is correct. This relates to the inputting of the data but ties into the next obligation in relation to storage limitation, where data is to be held for a prolonged period, organisations should periodically check with the Data Owner that the Personal Data remains current.

Storage Limitation	Personal Data should only be held for as long as it is needed to serve the Purpose.
Integrity and Confidentiality	Personal Data should be held in a secure way and this applies to both paper and digitally held data. The Council have attained the GovConnect standard and also undertake periodic penetration testing and can as a result demonstrate compliance. In addition Information Security Framework provides additional steps for staff to take to ensure data integrity and maintain confidentiality.
Accountability	Organisations are obliged to be accountable to Data Owners for any breach.

DEMONSTRATING COMPLIANCE

18. This will be delivered in 3 ways

Robust Policies and Processes

19. Attached to this report at Appendix 1 are the following policies

a. Data Breach Policy

As an organisation we store, process, and share a large amount of personal information. Data is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage or detrimental effect on the organisation.

We are obliged under the Data Protection Act and the GDPR to have a process in place designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

b. Data Retention and Erasure Policy

The purpose of this policy is to ensure that necessary data, records and documents for the Council are adequately protected and maintained and to ensure that records that are no longer needed or are of no value are discarded at the proper time. This policy is also for the purpose of aiding Council employees in understanding their obligations in retaining data or electronic documents including email, web files, text files, sound and movie files, PDF documents and all Microsoft Office or other formatted files.

In summary, personal data will be retained for no longer than is necessary. A Data Retention Schedule will be produced by the Council to demonstrate a generic retention period based on the purpose of the data and data retention guidelines. Each Service within the Council will also produce its own Data Retention Schedule specific to its service.

In the event that the retention of personal data is no longer necessary for the operation of [the Council the data shall be deleted and all copies shall be destroyed as per the defined schedule.

c. Information Classification Policy

The Council recognise that information is a vital asset to the organisation and take our responsibilities under the GDPR seriously. All of our activities create information assets in

one form or another. This Information Asset Classification Policy is concerned with managing the information assets of the Council.

The purpose of this Data Classification Policy is to ensure:

- Availability, integrity and confidentiality are provided at the necessary levels for all identified data assets
- Return on investment by implementing controls where they are needed the most
- Map data protection levels with organisational needs and the need to protect personal data
- Mitigate threats of unauthorised access and disclosure
- Comply with legal and regulation requirements

d. Information Security Policy

We all hold personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. An information security system within the Council is aimed at protecting employees, partners and customers of the company from illegal or damaging actions by individuals, either directly or implied, knowingly or unknowingly, when processing information and data which come at their disposal, as well as using certain equipment for fulfilment of their work duties.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access to in the course of their work.

The policy shall apply to processing of information within any systems or held on any media involved in the data/information processing within the company, irrespective of whether data/information processing is related to internal business operations of the company or to external relations of the company with any third parties.

e. Privacy Standard (GDPR) (formerly known as the Data Protection Policy)

This is an internal-facing privacy standard (previously, a data protection policy) setting out the principles and legal conditions that the Council must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of their operations and activities, including customer, supplier and employee data. It is tailored to comply with the General Data Protection Regulation ((EU) 2016/679) (GDPR) and replaces Standard document, Data protection policy.

f. Data Usage Policy

Changes in technology have resulted in us communicating and gathering information from our stakeholders via many new methods. The majority of our data gathering is now done so electronically.

The purpose of this policy is to identify appropriate and inappropriate use of data and to ensure Chorley Council meets its requirements of advising data subjects of rights available to them. We must inform individuals:

- how we will process their data
- if their data will be shared
- of the rights they are entitled to
- the required contact details
- how long data will be stored for
- whether submission of personal data is a statutory or contractual requirement

• of any automated decision making take place

The objective of this policy is to create a set of guidelines that will detail: the information we need to provide to individuals when they provide personal information to us, or the information we will communicate to individuals when we receive their data via another channel; and when and how the information will be communicated

g. General Privacy Notice (For external use/customers for the website and for each building)

The Council is a public authority and has certain powers and obligations. Most of the personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the Council's services. This privacy notice sets out our residents and customers rights and the Council's obligations to you.

Being transparent and providing accessible information to individuals about how you will use their personal data is a key element of the Data Protection Act 1998 (DPA) and the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

h. Privacy Notice (For Staff, Councillors and Role holders)

This is the same as above but this Privacy notice is specifically for employees and Councillors at the Council so the above is applicable here.

These have been prepared in accordance with the requirements of GDPR and using the Data Protection by Design and Default principles set out the ICO. These policies set out the overarching corporate position on Data Protection. Members are being asked to approve and adopt these policies. They will ensure that the Council complies with its obligations under the Principles and can deliver assurance to Data Owners when they exercise their rights.

20. Members are advised that teams and services will consider fixing specific data retention periods for the Personal Data they hold. These will be documented and held centrally.
21. Compliance with the Policies and Processes will ensure the Council are compliant with the requirements of GDPR.

Training

22. Whilst Data Controllers are required to ensure their teams have knowledge of their policies and the procedures, mandatory training is being provided to all staff through an online module on the Council's elearning platform. Officers without access will be having face to face training.
23. This will provide an understanding of the Data Protection Principles and Rights and enable staff to better understand the requirements of the policies.
24. Where training has been provided and there are clear policies and procedures to follow, the Council will have a defence against a Data Breach by a Data Processor.
25. After the enacting of the new Data Protection Act this year, additional face to face training will be provided to Data Controllers and other senior staff.

Continuous Monitoring and the Data Protection Officer

26. In order to demonstrate compliance the Council will implement a monitoring regime which will assess both the compliance with policies but also the continued suitability of the policies adopted.
27. This regime will be overseen by the Data Protection Officer. This is a post which must be independent to the setting of Council Data Protection Policies, must report into the Senior Management Team and have a recognised GDPR qualification.
28. It is proposed this function be discharged by the Council's Monitoring Officer.

IMPLICATIONS OF REPORT

29. This report has implications in the following areas and the relevant Directors' comments are included:

Finance		Customer Services	
Human Resources		Equality and Diversity	
Legal	X	Integrated Impact Assessment required?	
No significant implications in this area		Policy and Communications	

COMMENTS OF THE STATUTORY FINANCE OFFICER

30. A budget has been provided to support the implementation of the GDPR. The proposals in this report do not have any financial consequences that are not contained within that budget.

COMMENTS OF THE MONITORING OFFICER

31. The Constitution requires that new policies are adopted by Council. The appointment of a Data Protection Officer is a requirement of the GDPR and necessary to ensure the COucnil are complaint. Adoption of the policies proposed will provide a framework to ensure that the Council operate a GDPR complaint environment.

REBECCA HUDDLESTON
DIRECTOR OF POLICY AND GOVERNANCE

There are no background papers to this report.

Report Author	Ext	Date	Doc ID
Chris Moister	5160	3 May 2018	

This page is intentionally left blank

Chorley Council

DATA BREACH POLICY

Version: 1 26.04.18

Background

The Council stores, process, and share a large amount of personal information. Data is a valuable asset that needs to be suitably protected. Every care is taken to protect personal data from incidents (either accidentally or deliberately) to avoid a data protection breach that could compromise security. Compromise of information, confidentiality, integrity, or availability may result in harm to individual(s), reputational damage or detrimental effect on the Council.

Aim

We are obliged under the Data Protection Act and the GDPR to have a process in place designed to ensure the security of all personal data during its lifecycle, including clear lines of responsibility. This policy sets out the procedure to be followed to ensure a consistent and effective approach is in place for managing data breach and information security incidents.

Scope

This Policy relates to all personal and sensitive data held by the Council Regardless of format.

This Policy applies to everyone at the Council. This includes temporary, casual or agency staff and contractors, consultants, suppliers and data processors working for, or on behalf of the Council.

The objective of this policy is to contain any breaches, to minimise the risk associated with the breach and consider what action is necessary to secure personal data and prevent further breaches.

Definition/Types of breach

For the purpose of this Policy, data security breaches include both confirmed and suspected incidents. An incident in the context of this policy is an event or action which may compromise the confidentiality, integrity or availability of systems or data, either accidentally or deliberately.

An incident includes but is not restricted to, the following:

- Loss or theft of confidential or sensitive data or equipment on which such data is stored (e.g. loss of laptop, USB stick, iPad/tablet device, or paper record)
- Equipment theft or failure
- Unauthorised use of, access to or modification of data or information systems
- Attempts (failed or successful) to gain unauthorised access to information or IT system
- Unauthorised disclosure of sensitive/confidential data
- Website defacement
- Hacking attack
- Unforeseen circumstances such as a fire or flood
- Human error
- ‘Blagging’ offences where information is obtained by deceiving the organisation who holds it

Reporting an incident

Any individual who accesses, uses or manages information is responsible for reporting data breach and information security incidents immediately to the appropriate manager using the form [attached].

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The report will include full and accurate details of the incident, when the breach occurred (dates and times), who is reporting it, if the data relates to people, the nature of the information and how many individuals are involved. An Incident Report Form should be completed as part of the reporting process. All staff should be aware that any breach may result in disciplinary procedures being instigated.

Containment and Recovery

Appropriate steps must be taken immediately to minimise the effect of the breach. An initial assessment will be made to establish the severity of the breach and to establish whether there is anything that can be done to recover any losses and limit the damage the breach could cause.

The investigation will need to take into account the following:

- The type of data involved
- Any sensitivity
- The protections that are in place (e.g. encryptions)
- What's happened to the data, has it been lost or stolen
- Whether the data could be put to any illegal or inappropriate use
- who the individuals are, number of individuals involved and the potential effects on those data subject(s)
- Whether there are wider consequences to the breach

Notification

Management should determine who needs to be notified of the breach. Every incident will be assessed on a case by case basis; however, the following will need to be considered:

- Whether there are any legal/contractual notification requirements
- Whether notification would assist the individual affected – could they act on the information to mitigate risks
- Whether notification would help prevent the unauthorised or unlawful use of personal data
- Would notification help the company meet its obligations under the seventh data protection principle;
- If a large number of people are affected, or there are very serious consequences
- Whether the Information Commissioner's Office (ICO) should be notified. The ICO will only be notified if personal data is involved. Guidance on when and how to notify ICO is available from their website at: https://ico.org.uk/media/1536/breach_reporting.pdf

All suspected and actual breaches should be recorded on the appropriate log to facilitate further evaluation and breach avoidance activity.

The dangers of over notifying

Not every incident warrants notification and over notification may cause disproportionate enquiries and work. Notification to the individuals whose personal data has been affected by the incident will include a description of how and when the breach occurred and the data involved. Specific and clear advice will be given on what they can do to protect themselves and include what action has already been taken to mitigate the risks. Individuals will also be provided with information on what has occurred.

Evaluation and response

Once the initial incident is contained, the organisation will carry out a full review of the causes of the breach; the effectiveness of the response(s) and whether any changes to systems, policies and procedures should be undertaken. Existing controls should be reviewed to determine their adequacy and whether any corrective action should be taken to minimise the risk of similar incidents occurring.

Data Retention and Erasure Policy

Version 1: 26th April 2018

INTRODUCTION

The Council accumulates vast amounts of data, of numerous types, including but not limited to, planning applications, claims, assets, correspondence, statements, legal documents, contracts, and financial records.

The data is held in a range of forms such as letters, emails, contracts, deeds, plans and can be physical ie hard copy or electronic.

Certain information may need to be retained for one or more of the following reasons:

- To meet operational needs,
- to fulfil statutory or other regulatory requirements,
- is evidence of agreements or events in the case of a dispute, or
- to preserve documents of historic or other value

Some of this information is personal data about living individuals.

The introduction of the General Data Protection Regulation (GDPR) now brings new requirements to consider relating to the retention of personal data, with the emphasis being around minimization of data (in terms of the volume of data held about individuals and the length of time that the data is held for). Data breaches carry considerable risk of reputational damage and financial penalties of up to €20 million.

Article 5(e) of the GDPR states that:

'personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purpose for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historic research purposes or statistical purposes in accordance with Article 89(1) subject to implication of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject ('storage limitation')

In addition to this, Recital 39 of the GDPR also states:

- *'In order to ensure that the personal data are not kept longer than necessary, time limits should be established by the controller for erasure or for a periodic review'*

Therefore, in order to meet our GDPR data retention obligations we need to ensure that:

- we are retaining information appropriately in order to fulfil our requirements, but
- we DO NOT retain personal data for longer than we are permitted to,

By having concise retention guidelines in place and ensuring that they are followed, will also remove the risk of personal data being processed after its permitted period (therefore removing a further risk), and ensures Chorley Council is meeting legal requirements (reducing the risk of financial fines being imposed as a result of breaches and the associated risks of reputational damage).

At the end of the retention period it is important to ensure that the information is disposed of in the most appropriate manner

Article 6(1) of the GDPR details lawfulness of processing and states that processing is lawful if at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

The lawfulness of processing being relied upon is an important factor when considering the retention period and must be taken into account.

DATA RETENTION APPROACH

The Council understands the importance of data being stored safely and for the correct period of time.

The creation of clear, concise guidelines will ensure that staff acting as Data Controllers understand the data retention requirements applicable to the data they decide the purpose and means of processing for and an appropriate data retention period can be determined and justified.

The Council will ensure personal data is securely disposed of when no longer needed.

The purpose of this policy is to ensure the Council is compliant with GDPR data retention obligations and will remain compliant in the future.

This policy will ensure that necessary data, records and documents the Council collate and hold are adequately protected and maintained and to ensure that records that are no longer needed or are of no value are discarded at the proper time. This policy is also for the purpose of aiding employees of the Council in understanding their obligations in retaining data or electronic documents including email, web files, text files, sound and movie files, PDF documents and all Microsoft Office or other formatted files.

In summary, personal data will be retained for no longer than is necessary. A Corporate Data Retention Schedule will be produced by the Council as well as individual teams within each Directorate to demonstrate a generic retention period based on the purpose of the data and data retention guidelines. Each Service within the Council will have its own Retention Schedule (as set out at Appendix 1) based on the data each team holds.

In the event that the retention of personal data is no longer necessary for the operation of the Council, the data shall be deleted and all copies shall be destroyed as per the defined schedule

POLICY OBJECTIVES

The objective of this policy is to assist officers of Chorley Council with the management, retention and disposal / destruction of records and information (particularly where personal information is included), held as either hard copy or held electronically:

- To ensure the Council operates in an appropriate manner that results in the Council meeting its legal obligations and thus remaining GDPR compliant
- To prevent premature destruction of information that needs to be retained for a specific period in order to satisfy a financial, legal or other requirement of public administration.

- To assist in identification of information that may have future value and is worth preserving for archival purposes.
- To promote an improved and consistent approach to data retention and destruction.

SCOPE

This policy applies to all personal information held by the Council and to all Council staff who handle documentation and process information.

POLICY STATEMENT

The Council will ensure that:

- it does not keep information for longer than is necessary
- it will retain the minimum amount of information required in order to carry out its statutory duties
- personal data is securely disposed of when no longer needed
- data will be disposed of in the most appropriate and agreed manner.

This will be achieved by Council staff adhering to the following:

- The retention of paper documents / hard copies will be kept to an absolute minimum.

- General files will no longer be allowed to be kept by staff. This is because they are impossible to interrogate once they have attained a certain size and is inefficient. GDPR asks Data Controllers to identify personal data and by keeping general files this will make it harder to be GDPR compliant. There is a risk that the Council will not be GDPR compliant.

- Wherever possible, paper documents (hard copies) will be scanned in and stored as a digital / electronic version and the paper (hard copy) will be disposed of in an appropriate manner (see below for further information). This will be carried out as quickly as possible after receipt of documents.
- Wherever possible, paper documents (hard copies) should not be kept on desks, lockers, drawers or trays.

- Unless specified otherwise in the Corporate Retention Policy, or any Service Retention Polices or documented Retention Schedules, paper documents / hard copies of documentation will be disposed of as follows:-

  - Contains confidential and commercially sensitive information - shredded onsite

  - Contains personal data – shredded onsite

  - Contains no confidential or personal data – disposed of in recycle (where possible) waste containers

  - Public documents, not containing confidential and / or personal information – disposed of in (recycle, where possible) waste containers

  - When documents are being disposed of on someone else's behalf, clear guidance should be provided as to how the documents should be disposed of, and in the absence of such guidance, documents should be shredded onsite.

- A register of destruction of records should be kept. Enough detail should he recorded to identify which records have been destroyed, it is not sufficient to record that a certain quantity of records was been destroyed on a particular date.

- If documents are to be shredded off-site by a 3rd party organisation, appropriate checks must have taken place to ensure their suitability to handle the data and arrangements documented. At the end of the data destruction process, the 3rd party organisation will supply on request, a Certificate of Destruction.

- Certain types of documents do not need to be, and indeed should not be retained at all wherever possible; this can include, unnecessary duplicated copies, trivial (normal course of business' type) emails, documents of no importance such as compliment slips, flyers, advertisements, compliment slips. It should be considered normal practice to dispose of these types of documents as soon as possible.
- Duplicated and superseded materials for instance, draft documents and minutes of meetings that have now been finalised can be destroyed without a retention period (and is deleted as 'normal course of business').

- The period for which personal data is stored should be limited to a strict minimum and time limits should be established by the data controller for deletion of the records (referred to as erasure in the GDPR) or for a periodic review. For further information regarding these time limits, please refer to Service specific Data Retention guidelines and Data Retention Schedule.

ADMINISTRATION

The following Record Retention Schedule is the initial maintenance, retention and disposal schedule for records held by the Council. This schedule should be reviewed regularly (every 6 months) to ensure the data retention policy approach is adhered to. The same applies to Service specific retention schedules.

There are certain occasions when information needs to be preserved beyond any limits set out in the policy. The policy must be SUSPENDED relating to a specific customer or document and the information retained beyond the period specified in this Data Retention Schedule in the following circumstances:

- Legal proceedings or a regulatory or similar investigation or obligation to produce information are known to be likely, threatened or actual
- A crime is suspected or detected
- Information is relevant to a company in liquidation, receivership or where a debt is due to the Council
- Information is considered by the owning unit to be of potential historical importance

In the case of possible or actual legal proceedings, investigations or crimes occurring, the type of information that needs to be retained relates to any that will help or harm the Council or the other side's case, liability or amount involved.

If there is any doubt over whether legal proceedings, an investigation or a crime could occur or what information material is relevant in these circumstances, the Council shall take such steps as is necessary to promptly inform all staff of any suspension in the further disposal of documents.

RESPONSIBILITES

The responsibilities of our people are detailed below:

Roles	Responsibility	Frequency
All officers	Ensure that any correspondence received via post, or delivered in person to the Council offices, is actioned. If the documentation needs to be retained, ensure that it is scanned	Ongoing

(All Directorates)	in and stored electronically on any appropriate CRM system and the paper copy of the document, is securely disposed of.	
	To action emails received from members of the public, or that contain personal information as soon as possible and to then delete the email once fully actioned (and no longer required). If the email needs to be retained, ensure that it is stored electronically on any appropriate CRM system and the original email deleted from officers mailbox.	Ongoing
	Ensure paper records are kept to an absolute minimum and to avoid storing in personal drawers, lockers, desk and trays wherever possible.	Ongoing
Line Managers / Team Leaders (All Directorates	Ensure staff are routinely reminded of the responsibilities covered above.	On-going
	Ensure staff receive training and support where appropriate	
Data Controllers / Information Asset Owners (All Directorates)	To be aware of regulatory requirements relating to the retention of data they collect and store	On-going
	To notify the GDPR Compliance Officer of statutory / regulatory changes that occur relating to the retention of the data held by their Directorate	On-going
	Ensure that all personal data is retained and disposed of, is done so in line with GDPR and statutory requirements.	On-going
HR Manager	To ensure HR / staff records are retained and disposed of, in line with GDPR and statutory requirements.	On-going
Health and Safety Officer	Ensuring that all Health and Safety records are retained and, when appropriate, disposed of in line with GDPR and statutory requirements.	On-going
Directors/Heads of Service	Ensuring that all teams are complying with GDPR; ensuring that Data Retention Schedules are completed; ensuring that the Council's suppliers and contractors demonstrate GDPR compliance and that they check their credentials and guarantees. As a controller the Council need to have a written contract that explicitly defines each parties responsibilities and liabilities. Importantly, data controllers are always liable for the compliance with GDPR. In addition, if the Council operate outside the EU the Council need to document the location of the controlling authority within the EU. Contracts with suppliers, verification and ongoing management are key to long term GDPR compliance.	On-going
Chief Executive	Overall Officer level responsibility for data retention	On-going
Audit	Work with ICT to review batch deletion to ensure it is functioning appropriately and that a suitable audit trail is	Annually

	recorded.	
	To carry out internal audits to ensure Services are adhering to policy, to report findings, and make recommendations for improvements that can be made	On-going
	Undertake spot checks as identified in the risk assessment	Ongoing
Policy & Communications	Ensuring that Marketing Strategies and Events are compliant with GDPR and keeping Staff updated.	On-going
ICT Manager	The Information Manager will have overall responsibility for maintaining systems capable of batch deletion of information that has reached its retention limit.	As required
	Work with Audit to review batch deletion to ensure it is functioning appropriately and that a suitable audit trail is recorded.	Annually

MONITORING AND REVIEW ARRANGEMENTS

This policy will be reviewed annually (or as required following legislative changes).

RECORD RETENTION SCHEDULE

The data retention policy is based on the following schedule.

DEPARTMENT / FUNCTION

A. Accounting and finance
B. Contracts
C. Corporate records
D. Correspondence and internal memoranda
E. Personal information
F. Electronic records
G. Insurance records
H. Legal
I. Miscellaneous
J. Personnel records
K. Tax records

A. Accounting and Finance

Record Type	Retention Period

Annual audit reports and financial statements	permanent
Annual audit records, including work papers and other documents that relate to the audit	7 years after completion of audit
Annual plans and budgets	2 years
Bank statements and cancelled cheques	7 years
Employee expense reports	7 years
Interim financial statements	7 years
Credit card records (documents showing customer credit card number)	2 years

All records showing customer bank details must be locked in a desk drawer or a filing cabinet when not in immediate use by staff. If it is determined that information on a document, which contains credit card information, is necessary for retention beyond 2 years, then the identifying details will be cut out of the document.

B. Contracts

Record type	**Retention Period**
Contracts and related correspondence (including any proposal that resulted in the contract and all other supportive documentation)	7 years after expiration or termination

C. Corporate Records

Record type	**Retention Period**
Corporate records (minutes, signed minutes of the board and all committees, record of incorporation, articles of incorporation,	permanent

annual corporate reports)	
Licenses and permits	permanent

D. Correspondence And Internal Memoranda

General principle: most correspondence and internal memoranda should be retained for the same period as the document to which they relate. For instance, a letter pertaining to a particular contract would be retained as long as the contract (7 years after expiration). It is recommended that records that support a particular project be kept with the project and take on the retention time of that particular project file.

Correspondence or memoranda that do not pertain to documents having a prescribed retention period should generally be discarded sooner. These may be divided into two general categories:

1. Those pertaining to routine matters and having no significant, lasting consequences should be discarded within two years. Some examples include:

- Routine letters and notes that require no acknowledgment or follow up, such as notes of appreciation, congratulations, letters of transmittal and plans for meetings
- Form letters that require no follow up
- Letters of general inquiry and replies that complete a cycle of correspondence
- Letters or complaints requesting specific action that have no further value after changes are made or action taken (such as name or address change)
- Other letters of inconsequential subject matter or that definitely close correspondence to which no further reference will be necessary
- Chronological correspondence files

Copies of interoffice correspondence and documents where a copy will be in the originating department file should be read and destroyed; unless that information provides reference to, or direction to other documents and must be kept for project traceability.

2. Those pertaining to non-routine matters or having significant lasting consequences should generally be permanently retained.

E. Retaining Personal Information

This section sets out the data retention policies and procedure that are designed to help ensure compliance with legal obligations in relation to the retention and deletion of personal information

Personal information that is processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The Council will usually delete personal data falling within the categories set out below at the date/time set out below:

Record type	**Retention period**
Information about a computer and about visits to and use of this website (including an IP address, geographical location, browser type and version, operating system, referral source, length of visit, page views and website navigation paths)	2 years following account closure
Information provided when registering with our website (including email address)	2 years following account closure
Information provided when completing a profile on our website (including a name, gender, date of birth, interests and hobbies, educational details)	2 years following account closure
Information provided for the purpose of subscribing to email notifications and/or newsletters (including a name and email address)	Indefinitely or until the client chooses to 'unsubscribe'
Information provided when using the services on the website or that is generated in the course of the use of those services (including the timing, frequency and pattern of service use)	Indefinitely
Information relating to any subscriptions made (including name, address, telephone number, email address and card details)	2 years following account closure
Information posted to our website for publication on the internet	2 years after post
Information contained in or relating to any communications sent through the website (including the communication content and metadata associated with the communication)	2 years following contact
Any other personal information chosen to be sent	2 years following contact

Notwithstanding the other provisions of this section, the Council will retain documents (including electronic documents) containing personal data:

- to the extent that we are required to do so by law;
- if we believe that the documents may be relevant to any ongoing or prospective legal proceedings;
- and in order to establish, exercise or defend our legal rights (including providing information to others for the purposes of fraud prevention and reducing credit risk).

The Council will run database backups of all electronic data contained on our servers. This backup will include all information relating to all current users, as well as any information that remains on the server due to any reason contained in this policy. This database backup is a safeguard to retrieve lost information within a one year retrieval period should system users experience any problems.

F. Electronic Documents

Electronic mail: not all email needs to be retained and, it depends on the subject matter.

- All emails from internal or external sources are to be deleted after 12 months
- Staff will strive to keep all but an insignificant minority of their emails related to business issues
- We will archive emails for six months after the staff have deleted it, after which time the email will be permanently deleted
- Staff will take care not to send confidential/proprietary information to outside sources

Electronic Documents: including Microsoft Office Suite and PDF files. Retention also depends on the subject matter.

- PDF documents - The length of time that a PDF file should be retained should be based upon the content of the file and the category under the various sections of this policy. The maximum period that a PDF file should be retained is 6 years. PDF files the employee deems vital to the performance of his or her job should be printed and stored in the employee's workspace
- Text/formatted files - Staff will conduct annual reviews of all text/formatted files (e.g., Microsoft Word documents) and will delete all those they consider unnecessary or outdated. After five years, all text files will be deleted from the network and the staff's desktop/laptop. Text/formatted files the staff deems vital to the performance of their job should be printed and stored in the staff's workspace

We do not automatically delete electronic files beyond the dates specified in this policy. It is the responsibility of all staff to adhere to the guidelines specified in this policy. In certain cases a document will be maintained in both paper and electronic form. In such cases the official document will be the electronic document.

G. Insurance Records

Record Type	Retention Period

Certificates	permanent
Claims files (including correspondence, medical records, injury documentation, etc.)	permanent
Insurance policies (including expired policies)	permanent

H. Legal Files and Papers

Record Type	Retention Period
Legal memoranda and opinions (including all subject matter files)	7 years after close of matter
Litigation files	1 year after expiration of appeals or time for filing appeals
Court orders	permanent
Contracts	10 years
Requests for departure from records retention plan	10 years
Register of Members	permanent
Minutes of Director’s meetings	10 years

I. Miscellaneous

Record Type	Retention Period

Consultant's reports	2 years
Material of historical value (including pictures, publications)	permanent
Policy and procedures manuals – original	Current version with revision history
Policy and procedures manuals copies	Retain current version only
Annual reports	permanent
Record of persons I.D. for money laundering purposes	5 years
Any work related reportable accident, injury or death	3 years from report
Immigration checks	2 years from termination of job

J. Personnel Records

Record Type	**Retention Period**
Job applications/interviews of unsuccessful candidates Note: Application forms should give the opportunity for subjects to object to their details being retained/processed.	6 months or less (longer with explicit consent).

Employee personnel records (including individual attendance records, annual leave, application forms, job or status change records, performance evaluations, termination papers, withholding information, garnishments, test results, training and qualification records)	6 years after separation
Employment contracts – individual	7 years after separation
Employment records correspondence with employment agencies and advertisements for job openings	3 years from date of hiring decision
Job descriptions	3 years after superseded
Working time opt-out forms	2 years
Current bank details of employees	Only as long as necessary

K. Tax Records

General Principle: Donors forum must keep books of account or records as are sufficient to establish amount of gross income, deductions, credits or other matters required to be shown in any such return. These documents and records shall be kept for as long as the contents thereof may become material in the administration of tax laws.

Record Type	Retention
Tax-exemption documents and related correspondence	permanent
Tax bills, receipts, statements	7 years
Tax returns	permanent
Sales/use of tax records	7 years
Annual information returns	permanent
Payroll/wage records for unincorporated businesses	5 years after 31 January following the year of assessment

PAYE records	3 years (minimum) from
Maternity records	3 years after the end of the tax year in which the maternity pay period ends

The above retention periods apply in all cases. The default retention period unless otherwise specified for any data item is 7 years, after which time the data should be securely deleted.

APPENDIX 1: DATA RETENTION SCHEDULE

Directorate / Service	Description of process	Record Type (Type of information / documents)	Retention period/ Action	Reason	Disposal / Destruction guidelines
CCTV Example	CCTV footage	Backup of CCTV footage	Deleted after 31 days	Common practice	Footage overwritten

Reason: Please detail if retention action is statutory or common practice (Standard practice followed by local authorities who are members of the Records Management Society); quote any other useful information such as relevant Acts.

Retention Period/Action: Please detail any statutory periods the data must be retained for, or quote agreed periods that data will be held for (eg, 1 yr after last administrative use). Please state “Permanently” for data that must be kept indefinitely, or for approximately 100 years, for legal and/or administrative purposes, and/or are of enduring value for historical research purposes.

Disposal / Destruction guidelines: Please detail how data is disposed once the Retention period is reached

This page is intentionally left blank

Chorley Council

Information Classification Policy

Version 1: 27th April 2018

What Does This Document Do?

This document defines the data classification schema used in your organisation.

How Often Do You Need To Update This Document?

You should review this document every 6 months to make sure you stay compliant.

Introduction

Chorley Council is committed to GDPR and data security. We recognise that information is a vital asset to any organisation and take our responsibilities under the GDPR seriously. All of our activities create information assets in one form or another. This Information Asset Classification Policy is concerned with managing the information assets of the Council.

The purpose of this Data Classification Policy is to ensure:

- Availability, integrity and confidentiality are provided at the necessary levels for all identified data assets
- Return on investment by implementing controls where they are needed the most
- Map data protection levels with organisational needs and the need to protect personal data
- Mitigate threats of unauthorised access and disclosure
- Comply with legal and regulation requirements

2. Principles

Information asset classification ensures that individuals who have a legitimate right to access a piece of information can do so, whilst also ensuring that assets are protected from those who have no right to access them. This policy ensures that correct classification and handling methods are applied and managed accordingly. This policy is based on the requirement that:

- All information assets must be handled and managed in accordance with their classification
- Information assets should be made available to all who have a legitimate need to access them
- The integrity of information must be maintained; information must also be accurate, complete, timely and consistent with other related information and events
- All individuals who have access to information assets, have a responsibility to handle them in accordance with their classification

3. Objectives of this Policy

- To define the responsibilities of individuals for safeguarding information assets
- To provide a rigorous and consistent classification system which ensures that information assets are appropriately protected and managed in accordance with UK legal requirements
- To minimise the damage to the organisation, its customers and partners as a result of sensitive information assets being intercepted or exposed
- To ensure that information assets which are lost, stolen, damaged or intercepted are sufficiently protected and unreadable so that unwarranted action cannot be taken against the organisation

4. Action Implementation

Procedures will be put in place to ensure that this policy is effective. These procedures include:

- Information users being appropriately identified and having access to information for which they have a legitimate need
- Information assets being appropriately managed and controlled in line with the requirements of this policy
- Information assets being identified and sufficiently protected in line with the correct categorisation and handling methods
- Ensuring that adequate control mechanisms are in place for protecting information assets
- Ensuring that information access control mechanisms are in place and that these mechanisms are reviewed regularly
- Ensuring that asset owners define the required physical security of computer rooms, networks, personal computers and procedures for computer maintenance

- Ensuring the safe disposal of all information assets and equipment

5. Data Protection Act 1998 (DPA) and The GDPR (2018)

The GDPR and DPA requires the organisation to ensure appropriate technical and organisational measures are taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of or damage to, personal data.

6. Asset Classification and Handling

Information assets that are sensitive or have value must be protected at all times. Consideration must be given to day to day activities and protection outside normal working hours.

All information must be classified into one of the following categories by those who own or are responsible for the information:

- Public
- Open
- Confidential
- Strictly Confidential
- Secret

A lot of information will fall into the *Public* or *Open* categories, but for good reason, such as personal privacy or protection of the Council's interests, some information assets may be categorised as "*Confidential"* or "*Strictly Confidential*".

In exceptional circumstances information may be classified as "*Secret".* In the event of uncertainty or disagreement as to the classification of the information asset, it is advised that the default category and handling methods should be Confidential or Strictly Confidential.

7. Asset Classification Categories, Type And Handling Methods

Category	**Type**	**Asset Handling Methods**
Public **Definition:** **May be viewed by anyone, anywhere in the world.**	**Public information assets may include but are not limited to:** • Principal contacts e.g. name/email address/telephone numbers for public-facing roles will be made freely available • Announcements from authorities • Publications • Press releases	**N.B some contacts are associated with specific job roles and responsibilities only and should not be released to the general public without consent.**
Open **Definition:** **Access is available to all.**	**Open information assets may include but are not limited to:** • Contacts e.g. name/email address/telephone number • "Approved" communications e.g. news/updates to ensure their relevance to day to day activities	**Secure handling may include but is not limited to:** Information should be formatted to enable basic security e.g. word documents converted into PDF to avoid tampering and disrepute. These include documents such as but not

	• Policies/procedures/ processes	limited to: • Procedures • Policies • Guidelines
Confidential **Definition:** **Access is limited to specified people with appropriate authorisation or on a need to know basis.**	**Confidential information assets may include but are not limited to:** • Personal details or identifiable information includes: (name/address/telephone number/email address/date of birth/National Insurance number/ ethnic or racial origin/religious beliefs, physical or mental health/sexual life/ political opinions/trade union membership/ the commission or alleged commission of criminal offences). • Information relating to the private wellbeing of a person • Wage slips • Death certificates • PDR documents • Employee contract data • Non-Disclosure Agreements • Documents in “draft “ format	**Secure handling may include but is not limited to:** **Paper Documents (In Transit/Rest)** • Secure storage - locked (files/folders/cabinets) • Approved third party courier • Use sealed envelopes instead of the usual transit envelopes • Secure disposal **Electronic Information assets (In transit/rest)** • Encryption • Password protection • SFTP (Secure file transfer protocol) • Secure file stores • Secure disposal • Reduced access rights/level of privileges

Strictly Confidential **Definition:** **Access is controlled and restricted to a small number of named individuals/ authorities**	**Strictly Confidential information assets may include but are not limited to:** • Bank details (sort code/account number) • Credit Card Details (PAN/CVV2/Expiry Date/PIN) • Financial data • Medical records • Servers • Server rooms • Usernames and passwords • Test data • Investigation	**Secure handling may include but is not limited to:** **Paper documents (In transit/rest)** • Secure storage - locked (files/folders/cabinets) • Approved third party courier • Use sealed envelopes instead of the usual transit envelopes **Electronic Information assets (In transit/rest)** • Encryption

	• Disciplinary proceedings • Submitted patents/IPR • Third party contract/supplier information **Infrastructure or network information (including hardware and software)**	• SFTP (secure file transfer protocol) • Secure file stores • Asset tags • Secure disposal • Access rights/Level of privileges
Secret **Definition:** **Access is subject to or obtained under the Official Secrets Act.**	**Special circumstances may require differing controls above/or below) local circumstances. Each requirement will be reviewed on a case by case basis in line with HMG controls.** **HMG advice and guidance is subject to regular change.**	

8. Classification Guidelines (Paper/Electronic Copy)

Classification markings must be clearly visible on all information assets containing a category of classification information. The appropriate markings are to appear clearly either at the top, in the centre or at the bottom of each page.

9. Re-classification of Information Assets

Some information assets may be reclassified from one category to another based on the content and intent of the asset. There must be sound reasoning for the reclassification. If there is any doubt over the classification of an asset, contact the Information Security Officer.

10. Sensitive Information Assets

10.1 Responsibility for definition and the appropriate protection of an information asset remains with the originator or owner.

10.2 A higher level of protection must be provided for sensitive information assets which includes 'personal data' and 'personal identifiable information', which is defined as data relating to ethnic or racial origin, religious beliefs, physical or mental health, sexual life, political opinions, trade union membership or the commission or alleged commission of criminal offences.

10.3 Identifying sensitive information is a matter for assessment in each individual case. Broadly speaking, information will be confidential if it is of limited public availability; is confidential in its very nature; has been provided on the understanding that it is confidential; and/or its loss or unauthorised disclosure could have one or more of the following consequences:

- Financial loss e.g. the withdrawal of a research grant or donation, a fine by the ICO or a legal claim for breach of confidence
- Reputational damage e.g. adverse publicity, demonstrations, complaints about breaches of privacy; and/or
- An adverse effect on the safety or well-being of staff of the organisation or those associated with it e.g. increased threats to staff engaged in sensitive work, embarrassment or damage to participants, benefactors and suppliers

11. Storage and Backup

It is the responsibility of each person to ensure sensitive data is stored, secured and backed up as per the required schedule. All sensitive data must be stored and secured via the approved and provided electronic/physical storage locations.

12. Data Anonymisation

All appropriate steps must be taken prior to disclosing, sharing or transferring information to ensure the anonymity of a data subject is undertaken and maintained in accordance with legislation.

Omitting/Redacting

Omitting or deleting specific personal identifiers is the most basic privacy method whereby sharing or releasing information removes personal data from any documents/records including omitting and redacting sensitive data.

Audio Visual/Verbal Exchange

Audio visual data and/or participant information can be difficult to anonymise due to the nature and format of the recordings. Audio visual and verbally exchanged recordings, where required, should be masked, edited and/or dubbed.

13. Secure Disposal

Information assets that are considered sensitive (i.e. Secret, Strictly Confidential or Confidential) and are no longer needed or are deemed to have reached “end of life” must be securely disposed of. There are several ways to dispose of information assets and equipment. For example: secure shredding (cross cut shredders).

14. Information Security Incident Response

In the event that an information asset is damaged or lost, this must be reported immediately to the appropriate manager and to the Information Security Manager.

This page is intentionally left blank

Chorley Council

Information Security Policy

Version 1: 27th April 2018

What does this document do?

This document is a data security policy. This is an important document and should be reviewed and discussed with everyone in the Council.

How often do you need to update this document?

You should review this document every 3 months to make sure you stay compliant.

Introduction

The Council holds personal data about our employees, clients, suppliers and other individuals for a variety of business purposes. An information security system within the Council is aimed at protecting employees, partners and customers of the Council from illegal or damaging actions by individuals, either directly or implied, knowingly or unknowingly, when processing information and data which come at their disposal, as well as using certain equipment for fulfilment of their work duties.

This policy sets out how we seek to protect personal data and ensure that staff understand the rules governing their use of personal data to which they have access to in the course of their work.

The policy shall apply to processing of information within any systems or held on any media involved in the data/information processing within the Council irrespective of whether data/information processing is related to internal business operations of the Council or to external relations of the Council with any third parties.

Scope

This policy applies to all staff. The Council may supplement or amend this policy with additional policies and guidelines from time to time.

Our Data Protection Officer has overall responsibility for the day-to-day implementation of this policy.

More details can be found in:

- **Data Retention and Erasure Policy**
- **Information Classification Policy**
- **International Data Transfer Procedures**

Business purposes

The purposes for which personal data may be used by us includes, but is not limited to:

Business purposes	Personnel, administrative, financial, regulatory, payroll and business development purposes. Business purposes include the following: - Compliance with our legal, regulatory and corporate governance obligations and good practice - Ensuring business policies are adhered to (such as policies covering email and internet use) - Operational reasons, such as recording transactions, training and quality control, ensuring the confidentiality of commercially sensitive information, security vetting, credit scoring and checking - Investigating complaints - Checking references, ensuring safe working practices, monitoring and managing staff access to systems and facilities and staff absences, administration and assessments

	- Monitoring staff conduct - Marketing our business - Improving services
Personal Data Information	relating to identifiable individuals, such as job applicants, current and former employees, agencies, contractors and other staff, clients, suppliers and marketing contacts Personal data we gather may include: individuals' contact details, educational background, financial and pay information, details of certificates and diplomas, education and skills, marital status, nationality, job title and CV
Sensitive Personal Data	Personal data about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health condition, criminal offences or related proceedings. Any use of sensitive personal data should be strictly controlled in accordance with this policy.

Any information/data which becomes available to the employees within performance of their work duties if related to Council and its operation, clients or cooperation partners, shall be deemed proprietary and confidential information of the Council thus being subject to protection in accordance with applicable laws and regulations regarding protection of confidential information, commercial/trade secrets and personal data.

Fair processing

We must process personal data fairly and lawfully in accordance with individuals' rights. This generally means that the Council should not process personal data unless the individual whose details we are processing has consented to this happening.

In most cases where we process sensitive personal data we will require the data subject's explicit consent to do this unless exceptional circumstances apply or we are required to do this by law (e.g. to comply with legal obligations to ensure Health And Safety at Work). Any such consent will need to clearly identify what the relevant data is, why it is being processed and to whom it will be disclosed.

We will ensure that any personal data we process is accurate, adequate, relevant but not excessive, given the purpose for which it was obtained. The Council will not process personal data obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

Roles and responsibilities

Data security is key to everything the Council does and is everyone's responsibility. In particular:

The Data Protection Officer's responsibilities:

- Keeping the board updated about data protection responsibilities, risks and issues
- Reviewing all data protection procedures and policies on a regular basis
- Arranging data protection training and advice for all staff members and those included in this policy
- Answering questions on data protection from staff, board members and other stakeholders
- Responding to individuals such as clients and employees who wish to know which data is being held on them by the Council
- Checking and approving with third parties that handle the Council's data, any contracts or agreement regarding data processing

Responsibilities of the IT Manager

- Ensuring all systems, services, software and equipment meet acceptable security standards
- Checking and scanning security hardware and software regularly to ensure it is functioning properly
- Researching third-party services (such as cloud services) that the Council is considering using to store or process data

Responsibilities of the Marketing Manager

- Approving data protection statements attached to emails and other marketing copy
- Addressing data protection queries from clients, target audiences or media outlets
- Coordinating with the DPO to ensure all marketing initiatives adhere to data protection law and the Council's data protection policy.

Data Security – Personal Responsibilities

It is the responsibility of everyone to keep personal data secure against loss or misuse. Where other organisations process personal data as a service on our behalf, the DPO will establish what, if any, additional specific data security arrangements need to be implemented in contracts with those third party organisations.

All staff will receive training on this policy. New joiners will receive training as part of the induction process. Further training will be provided whenever there is a substantial change in the law or to our policy and procedure. Completion of training is compulsory.

The Council takes compliance of this policy very seriously. Failure to comply puts both you and the Council at risk.

The importance of this policy means that failure to comply with any requirement may lead to disciplinary action under our procedures which may result in dismissal. If you have any questions or concerns about anything in this policy, do not hesitate to contact your manager.

Security Policies

Data Storage

- All data and information collected and processed in any form (paper, electronic etc) shall be subject to the requirements of this policy. Any statutory regulation in respect to collection, processing, protection and retention of data/information and such documents shall be stored in safe place as designated by the Council for a retention period provided for by applicable laws and/or indicated by the Council

- Employees are not permitted to keep any confidential information on their devices except information which is temporarily needed for specific, work related activity. Any download of such files to local devices should be avoided and limited only to necessity related with information processing for work purposes

- Internet access and operations performed by employees according to requirements of the applicable laws and regulations may be filtered and monitored by duly authorised IT personnel of the Council

- Any mobile, portable devices (including laptops, tablets, smartphones and other handheld computing devices) as well any cloud information storage places should be approved by IT personnel of the Council and secured to prevent unauthorised access

- Only systems and program software licensed and authorised by the Council can be installed and used on equipment and tools used within the Council. Before downloading or installing any software to devices held and used by employees for the purposes described in this policy permission from the IT personnel shall be obtained

- In cases when employees use home devices for access to corporate resources of the Coucil (e.g. CRM, email, online/cloud databases) the employees shall be obliged to comply with the requirements of this policy; equally as if they were using equipment provided by the Council. Accordingly, it shall be prohibited to store any data and information related to the Council on the device; any processing of the data shall be permitted only through cloud and online storage places used by the Council

- It shall be strictly prohibited to use public access devices at all times (e.g. at internet cafes, libraries etc). Unless it is critical and urgent work and a direct manager of the employee has provided explicit written consent for such action

- In case access is granted to the employee to a files storage system of a client or the Council; the employee shall be obliged to use the access tools provided by the client or Council and follow provided guidelines on secure information/data processing requirements (including use of encryption systems, passwords, data use limitations, using dedicated locations etc)

- No information/data referred to in this policy shall be sent, forwarded or otherwise submitted to any third party, unless it is necessary for the accomplishment of work duties of the employee. In case of forwarding and submission of data to third parties it shall be ensured that the data is protected and corresponding security measures have been taken

- The Council shall audit the systems used in processing of information/data to control ongoing compliance with this policy and applicable statutory requirements

Data Retention

The Council must retain personal data for no longer than is necessary. What is necessary will depend on the circumstances of each case, taking into account the reasons why that personal data was obtained, but should be determined in a manner consistent with our data retention guidelines. For more information refer to the data retention and erasure policy document.

Encryption and Anonymisation Policy

Encryption protects information stored on mobile and static devices and in transmission. It is a way of safeguarding against unauthorised or unlawful processing of data. There are a number of different encryption options available.

Anonymisation of personal data should be considered where possible and desirable. Anonymisation ensures the availability of rich data resources, whilst protecting individuals' personal data.

The Council will consider encryption alongside other technical measures, taking into account the benefits and risks that it can offer. Appropriate technical and organisational measures will be taken against unauthorised or unlawful processing of personal data and against accidental loss, destruction or damage to personal data.

Transferring Data Internationally

There are restrictions on international transfers of personal data. You must not transfer personal data anywhere outside the UK without first consulting the Data Protection Officer. For more information refer to the International data transfer procedures document.

Prohibited Activities

Save for exceptions specifically established; in no case and under no circumstances should any equipment, systems or tools owned by the Council, its clients or partners be used for purposes not related to work duties of the employee or not related to business operation of the Council.

The following activities are prohibited, with no exceptions. A breach of this policy can lead to disciplinary action and other legal action.

- Violation of the rights of any person or Council protected by intellectual property rights, including but not limited to installation, copying, distribution or storage on any Council systems or equipment of any illegal software, online platforms, any other electronic contents which is not licensed for use of by the Council
- Unauthorised copying of materials subject to copyright protection
- Violation of the rights of any person by excessive and unnecessary collection and processing of personal data
- Accessing data, server or an account for the purpose other than conducting business operation of the Council or performance of work duties of the particular Employee
- Exporting of software, technical information, encryption software or technology in breach of applicable international or national laws and regulations and/or directions of the Council
- Exporting of any data or information which is of proprietary and/or confidential value to the Council, if such exporting is not required in the course of business operation of the Council or performance of work duties of the employee and/or is in breach of internal regulations of the Council, applicable laws or regulations
- Revealing employee's account password to others and allowing use of such account by others (including but not limited to employee's family members)
- Making fraudulent offers of products, items or services originating from the Council's account
- Effecting security breaches or disruptions of network communication. Such security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account which the employee is not expressly authorised to access, unless such access rights are granted to the employee due to him/her being involved in a specific project of the Council
- Using any program/script/command or sending message of any kind with intent to interfere with or disable a user session via any means

Reporting Security Incidents

- All information/data processing security incidents or threatened incidents shall be immediately reported to management, which accordingly shall take all measures for prevention of potential damage, elimination of the damage caused and restitution of previous security status
- If applicable, it shall be the obligation of the management to ensure further reporting on data/information security breach to all relevant authorities and individuals involved as provided for by applicable laws and regulations and/or laws of the European Union

Review

This document should be reviewed and amended regularly to ensure compliance.

Privacy Standard (GDPR version) (Data Protection Policy)

Version 1: 30th April 2018

Privacy standard (GDPR version)

This is an internal-facing privacy standard (previously, a data protection policy) setting out the principles and legal conditions that the Council must satisfy when obtaining, handling, processing, transporting or storing personal data in the course of their operations and activities, including customer, supplier and employee data. It is tailored to comply with the General Data Protection Regulation ((EU) 2016/679) (GDPR) and replaces Standard document, Data protection policy.

The GDPR will take effect on May 2018 and guidance is still being issued. The Privacy Standard may be amended as and when further guidance is published.

Further amendments may be made to this document when the Article 29 Working Party's final Guidelines on Transparency under the GDPR (WP260) are published.

1. INTERPRETATION

1.1 DEFINITIONS:

Automated Decision-Making (ADM): when a decision is made which is based solely on Automated Processing (including profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

Automated Processing: any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

Council name:

Council Personnel: all employees, workers [contractors, agency workers, consultants,] directors, members and others.

Consent: agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signifies agreement to the Processing of Personal Data relating to them.

Data Controller: the person or organisation that determines when, why and how to process Personal Data. It is responsible for establishing practices and policies in line with the GDPR. We are the Data Controller of all Personal Data relating to our Council Personnel and Personal Data used in our business for our own commercial purposes.

Data Subject: a living, identified or identifiable individual about whom we hold Personal Data. Data Subjects may be nationals or residents of any country and may have legal rights regarding their Personal Data.

Data Privacy Impact Assessment (DPIA): tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

Data Protection Officer (DPO): the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a DPO or refers to the Council data privacy team with responsibility for data protection compliance.

EEA: the 28 countries in the EU, and Iceland, Liechtenstein and Norway.

Explicit Consent: consent which requires a very clear and specific statement (that is, not just action).

General Data Protection Regulation (GDPR): the General Data Protection Regulation ((EU) 2016/679). Personal Data is subject to the legal safeguards specified in the GDPR.

Personal Data: any information identifying a Data Subject or information relating to a Data Subject that we can identify (directly or indirectly) from that data alone or in combination with other identifiers we possess or can reasonably access. Personal Data includes Sensitive Personal Data and Pseudonymised Personal Data but excludes anonymous data or data that has had the identity of an individual permanently removed. Personal data can be factual (for example, a name, email address, location or date of birth) or an opinion about that person's actions or behaviour. Personal Data specifically includes, but is not limited to

- Names, titles and aliases, photogaphs
- Contact details such as telephone numbers, addresses, and email addresses
- Gender, age, marital status, nationality, education/work histories, academic/professional qualifications, hobbies, family composition, and dependents
- Financial identifiers such as bank account numbers, payments, payment/transaction identifiers, policy numbers and claim numbers

Personal Data Breach: any act or omission that compromises the security, confidentiality, integrity or availability of Personal Data or the physical, technical, administrative or organisational safeguards that we or our third-party service providers put in place to protect it. The loss, or unauthorised access, disclosure or acquisition, of Personal Data is a Personal Data Breach.

Privacy by Design: implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

Privacy Guidelines: the Coouncil's privacy/GDPR related guidelines provided to assist in interpreting and implementing this Privacy Standard and Related Policies, available here: [INSERT LINK TO LIST OF BUSINESS SPECIFIC GUIDELINES OR SET OUT THESE GUIDELINES IN AN APPENDIX].

Privacy Notices (also referred to as Fair Processing Notices) or Privacy Policies: separate notices setting out information that may be provided to Data Subjects when the Council collects information about them. These notices may take the form of general privacy statements applicable to a specific group of individuals (for example, employee privacy notices or the website privacy policy) or they may be stand-alone, one time privacy statements covering Processing related to a specific purpose.

Processing or Process: any activity that involves the use of Personal Data. It includes obtaining, recording or holding the data, or carrying out any operation or set of operations on the data including organising, amending, retrieving, using, disclosing, erasing or destroying it. Processing also includes transmitting or transferring Personal Data to third parties.

Pseudonymisation or Pseudonymised: replacing information that directly or indirectly identifies an individual with one or more artificial identifiers or pseudonyms so that the person, to whom the data relates, cannot be identified without the use of additional information which is meant to be kept separately and secure.

Related Policies: the Council's policies, operating procedures or processes related to this Privacy Standard and designed to protect Personal Data, available here: [INSERT LINK TO LIST OF BUSINESS SPECIFIC POLICIES OR SET OUT THESE POLICIES IN AN APPENDIX].

Sensitive Personal Data: information revealing racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health conditions, sexual life, sexual orientation, biometric or genetic data, and Personal Data relating to criminal offences and convictions.

2. INTRODUCTION

The Council are committed to a policy of protecting the rights and privacy of individuals. We need to collect and use certain types of Data in order to carry on our work. This personal information must be collected and dealt with appropriately. The Data Protection Act 1998 (DPA) governs the use of information about people (personal data). Personal data can be held on computers, laptops and mobile devices, or in a manual file, and includes email, minutes of meetings, and photographs. The Council will remain the data controller for the information held. The staff and anyone employed within the Council will be personally responsible for processing and using personal information in accordance with the Data Protection Act. Staff, volunteers and anyone who has access to personal information, will be expected to read and comply with this policy.

The purpose of this policy is to set out the Council's commitment and procedures for protecting personal data. The Council regards the lawful and correct treatment of personal information as very important to successful working, and to maintaining the confidence of those with whom we deal with.

This Privacy Standard sets out how Chorley Council ("the Council") handle the Personal Data of our customers, suppliers, employees, workers and other third parties.

This Privacy Standard applies to all Personal Data we Process regardless of the media on which that data is stored or whether it relates to past or present employees, workers, customers, clients or supplier contacts, shareholders, website users or any other Data Subject.

This Privacy Standard applies to all Council Personnel ("you", "your"). You must read, understand and comply with this Privacy Standard when Processing Personal Data on our behalf and attend training on its requirements. This Privacy Standard sets out what we expect from you in order for the Council to comply with applicable law. Your compliance with this Privacy Standard is mandatory. Related Policies and Privacy Guidelines are available to help you interpret and act in accordance with this Privacy Standard. You must also comply with all such Related Policies and Privacy Guidelines. Any breach of this Privacy Standard may result in disciplinary action.

This Privacy Standard (together with Related Policies and Privacy Guidelines) is an internal document and cannot be shared with third parties, clients or regulators without prior authorisation from the DPO.

3. SCOPE

The Council recognise that the correct and lawful treatment of Personal Data will maintain confidence in the organisation and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times. The Council is exposed to potential fines of up to EUR20 million (approximately £18 million), whichever is higher and depending on the breach, for failure to comply with the provisions of the GDPR.

All staff, including individual business areas, departments, supervisors, managers and directors are responsible for ensuring all Council Personnel comply with this Privacy Standard and need to implement appropriate practices, processes, controls and training to ensure such compliance.

The DPO is responsible for overseeing this Privacy Standard and, as applicable, developing Related Policies and Privacy Guidelines. That post is held by Chris Moister, Head of Policy and Governance, 01257 515160, Chris.Moister@chorley.gov.uk.

Please contact the DPO with any questions about the operation of this Privacy Standard or the GDPR or if you have any concerns that this Privacy Standard is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

(a) if you are unsure of the lawful basis which you are relying on to process Personal Data (including the legitimate interests used by the Council) (see Section 5.1 below);

(b) if you need to rely on Consent and/or need to capture Explicit Consent (see Section 5.2 below);

(c) if you need to draft Privacy Notices or Fair Processing Notices (see Section 5.3 below);

(d) if you are unsure about the retention period for the Personal Data being Processed (see Section [9] below);

(e) if you are unsure about what security or other measures you need to implement to protect Personal Data (see Section [10.1] below);

(f) if there has been a Personal Data Breach (Section [10.2] below);

(g) if you are unsure on what basis to transfer Personal Data outside the EEA (see Section [11] below);

(h) if you need any assistance dealing with any rights invoked by a Data Subject (see Section [12]);

(i) whenever you are engaging in a significant new, or change in, Processing activity which is likely to require a DPIA (see Section [13.4] below) or plan to use Personal Data for purposes others than what it was collected for;

(j) If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making (see Section [13.5] below);

(k) If you need help complying with applicable law when carrying out direct marketing activities (see Section [13.6] below); or

(l) if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors) (see Section [13.7] below).

4. PERSONAL DATA PROTECTION PRINCIPLES

The Council adhere to the principles relating to Processing of Personal Data set out in the GDPR which require Personal Data to be:

(a) Processed lawfully, fairly and in a transparent manner (Lawfulness, Fairness and Transparency).

(b) Collected only for specified, explicit and legitimate purposes (Purpose Limitation).

(c) Adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed (Data Minimisation).

(d) Accurate and where necessary kept up to date (Accuracy).

(e) Not kept in a form which permits identification of Data Subjects for longer than is necessary for the purposes for which the data is Processed (Storage Limitation).

(f) Processed in a manner that ensures its security using appropriate technical and organisational measures to protect against unauthorised or unlawful Processing and against accidental loss, destruction or damage (Security, Integrity and Confidentiality).

(g) Not transferred to another country without appropriate safeguards being in place (Transfer Limitation).

(h) Made available to Data Subjects and Data Subjects allowed to exercise certain rights in relation to their Personal Data (Data Subject's Rights and Requests).

The Council are responsible for and must be able to demonstrate compliance with the data protection principles listed above (Accountability).

5. LAWFULNESS, FAIRNESS, TRANSPARENCY

5.1 LAWFULNESS AND FAIRNESS

Personal data must be Processed lawfully, fairly and in a transparent manner in relation to the Data Subject.

The Council may only collect, Process and share Personal Data fairly and lawfully and for specified purposes. The GDPR restricts our actions regarding Personal Data to specified lawful purposes. These restrictions are not intended to prevent Processing but ensure that we Process Personal Data fairly and without adversely affecting the Data Subject.

The GDPR allows Processing for specific purposes, some of which are set out below:

(a) the Data Subject has given his or her Consent;

(b) the Processing is necessary for the performance of a contract with the Data Subject;

(c) to meet our legal compliance obligations.;

(d) to protect the Data Subject's vital interests;

(e) to pursue our legitimate interests for purposes where they are not overridden because the Processing prejudices the interests or fundamental rights and freedoms of Data Subjects. The purposes for which we process Personal Data for legitimate interests need to be set out in applicable Privacy Notices or Fair Processing Notices; or

(f) OTHER GDPR PROCESSING GROUNDS.

You must identify and document the legal ground being relied on for each Processing activity in accordance with the Council's guidelines on Lawful Basis for Processing Personal Data.

5.2 CONSENT

A Data Controller must only process Personal Data on the basis of one or more of the lawful bases set out in the GDPR, which include Consent.

A Data Subject consents to Processing of their Personal Data if they indicate agreement clearly either by a statement or positive action to the Processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. If Consent is given in a document which deals with other matters, then the Consent must be kept separate from those other matters.

Data Subjects must be easily able to withdraw Consent to Processing at any time and withdrawal must be promptly honoured. Consent may need to be refreshed if you intend to Process Personal Data for a different and incompatible purpose which was not disclosed when the Data Subject first consented.

Unless the Council can rely on another legal basis of Processing, Explicit Consent is usually required for Processing Sensitive Personal Data, for Automated Decision-Making and for cross border data transfers. Usually we will be relying on another legal basis (and not require Explicit Consent) to Process most types of Sensitive Data. Where Explicit Consent is required, you must issue a Fair Processing Notice to the Data Subject to capture Explicit Consent.

The Council will need to evidence Consent captured and keep records of all Consents so that the Council can demonstrate compliance with Consent requirements.

5.3 TRANSPARENCY (NOTIFYING DATA SUBJECTS)

The GDPR requires Data Controllers to provide detailed, specific information to Data Subjects depending on whether the information was collected directly from Data Subjects or from elsewhere. Such information must be provided through appropriate Privacy Notices or Fair Processing Notices which must be concise, transparent, intelligible, easily accessible, and in clear and plain language so that a Data Subject can easily understand them.

Whenever we collect Personal Data directly from Data Subjects, including for human resources or employment purposes, we must provide the Data Subject with all the information required by the GDPR including the identity of the Data Controller and DPO, how and why we will use, Process, disclose, protect and retain that Personal Data through a Fair Processing Notice which must be presented when the Data Subject first provides the Personal Data..

When Personal Data is collected indirectly (for example, from a third party or publically available source), you must provide the Data Subject with all the information required by the GDPR as soon as possible after collecting/receiving the data. You must also check that the Personal Data was collected by the third party in accordance with the GDPR and on a basis which contemplates our proposed Processing of that Personal Data.

You must comply with the Council's guidelines on drafting Privacy Notices/Fair Processing Notices.

6. PURPOSE LIMITATION

Personal Data must be collected only for specified, explicit and legitimate purposes. It must not be further Processed in any manner incompatible with those purposes.

You cannot use Personal Data for new, different or incompatible purposes from that disclosed when it was first obtained unless you have informed the Data Subject of the new purposes and they have Consented where necessary.

7. DATA MINIMISATION

Personal Data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is Processed.

You may only Process Personal Data when performing your job duties requires it. You cannot Process Personal Data for any reason unrelated to your job duties.

You may only collect Personal Data that you require for your job duties: do not collect excessive data. Ensure any Personal Data collected is adequate and relevant for the intended purposes.

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Council's data retention guidelines.

8. ACCURACY

Personal Data must be accurate and, where necessary, kept up to date. It must be corrected or deleted without delay when inaccurate.

You will ensure that the Personal Data we use and hold is accurate, complete, kept up to date and relevant to the purpose for which we collected it. You must check the accuracy of any Personal Data at the point of collection and at regular intervals afterwards. You must take all reasonable steps to destroy or amend inaccurate or out-of-date Personal Data.

9. STORAGE LIMITATION

Personal Data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed.

You must not keep Personal Data in a form which permits the identification of the Data Subject for longer than needed for the legitimate business purpose or purposes for which we originally collected it including for the purpose of satisfying any legal, accounting or reporting requirements.

The Council will maintain retention policies and procedures to ensure Personal Data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time. You must comply with the Council's guidelines on Data Retention and comply with Directorate Data Rentention Policies.

Council Personnel will take all reasonable steps to destroy or erase from Council systems all Personal Data that we no longer require in accordance with all the Council's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

Council personnel will ensure Data Subjects are informed of the period for which data is stored and how that period is determined in any applicable Privacy Notice or Fair Processing Notice.

10. SECURITY INTEGRITY AND CONFIDENTIALITY

10.1 PROTECTING PERSONAL DATA

Personal Data must be secured by appropriate technical and organisational measures against unauthorised or unlawful Processing, and against accidental loss, destruction or damage.

The Council will develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of Personal Data that we own or maintain on behalf of others and identified risks (including use of encryption and Pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our Processing of Personal Data. Council Personnel are responsible for protecting the Personal Data we hold. Council Personnel must implement reasonable and appropriate security measures against unlawful or unauthorised Processing of Personal Data and against the accidental loss of, or damage to, Personal Data. You must exercise particular care in protecting Sensitive Personal Data from loss and unauthorised access, use or disclosure.

Council Personnel must follow all procedures and technologies we put in place to maintain the security of all Personal Data from the point of collection to the point of destruction. You may only transfer Personal Data to third-party service providers who agree to comply with the required policies and procedures and who agree to put adequate measures in place, as requested.

You must maintain data security by protecting the confidentiality, integrity and availability of the Personal Data, defined as follows:

(a) Confidentiality means that only people who have a need to know and are authorised to use the Personal Data can access it.

(b) Integrity means that Personal Data is accurate and suitable for the purpose for which it is processed.

(c) Availability means that authorised users are able to access the Personal Data when they need it for authorised purposes.

You must comply with all applicable aspects of our Information Security Program and Framework and Information Security Policy OR comply with and not attempt to circumvent the administrative, physical and technical safeguards we implement and maintain in accordance with the GDPR and relevant standards to protect Personal Data.

10.2 REPORTING A PERSONAL DATA BREACH

The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

We have put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where we are legally required to do so.

If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches [the DPO, the information technology or security department, the legal department and follow the

Security Incident Response Plan/Checklist. You should preserve all evidence relating to the potential Personal Data Breach.

11. TRANSFER LIMITATION

The GDPR restricts data transfers to countries outside the EEA in order to ensure that the level of data protection afforded to individuals by the GDPR is not undermined. You transfer Personal Data originating in one country across borders when you transmit, send, view or access that data in or to a different country.

You may only transfer Personal Data outside the EEA if one of the following conditions applies:

(a) the European Commission has issued a decision confirming that the country to which we transfer the Personal Data ensures an adequate level of protection for the Data Subjects' rights and freedoms;

(b) appropriate safeguards are in place such as binding corporate rules (BCR), standard contractual clauses approved by the European Commission, an approved code of conduct or a certification mechanism, a copy of which can be obtained from the DPO;

(c) the Data Subject has provided Explicit Consent to the proposed transfer after being informed of any potential risks; or

(d) the transfer is necessary for one of the other reasons set out in the GDPR including the performance of a contract between us and the Data Subject, reasons of public interest, to establish, exercise or defend legal claims or to protect the vital interests of the Data Subject where the Data Subject is physically or legally incapable of giving Consent and, in some limited cases, for our legitimate interest.

You must comply with the Council's guidelines on cross border data transfers.

12. DATA SUBJECT'S RIGHTS AND REQUESTS

Data Subjects have rights when it comes to how we handle their Personal Data. These include rights to:

(a) withdraw Consent to Processing at any time;

(b) receive certain information about the Data Controller's Processing activities;

(c) request access to their Personal Data that we hold;

(d) prevent our use of their Personal Data for direct marketing purposes;

(e) ask us to erase Personal Data if it is no longer necessary in relation to the purposes for which it was collected or Processed or to rectify inaccurate data or to complete incomplete data;

(f) restrict Processing in specific circumstances;

(g) challenge Processing which has been justified on the basis of our legitimate interests or in the public interest;

(h) request a copy of an agreement under which Personal Data is transferred outside of the EEA;

(i) object to decisions based solely on Automated Processing, including profiling (ADM);

(j) prevent Processing that is likely to cause damage or distress to the Data Subject or anyone else;

(k) be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms;

(l) make a complaint to the supervisory authority; and

(m) in limited circumstances, receive or ask for their Personal Data to be transferred to a third party in a structured, commonly used and machine readable format.

You must verify the identity of an individual requesting data under any of the rights listed above (do not allow third parties to persuade you into disclosing Personal Data without proper authorisation).

You must immediately forward any Data Subject request you receive to your supervisor OR the DPO and comply with the Council's Data Subject response process.

13. ACCOUNTABILITY

13.1 The Data Controller must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The Data Controller is responsible for, and must be able to demonstrate, compliance with the data protection principles.

The Council must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO (where necessary) and an executive accountable for data privacy;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Privacy Standard, Related Policies, Privacy Guidelines, Privacy Notices or Fair Processing Notices;

(d) regularly training Council Personnel on the GDPR, this Privacy Standard, Related Policies and Privacy Guidelines and data protection matters including, for example, Data Subject's rights, Consent, legal basis, DPIA and Personal Data Breaches. The Council must maintain a record of training attendance by Council Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

13.2 RECORD KEEPING

The GDPR requires us to keep full and accurate records of all our data Processing activities.

You must keep and maintain accurate corporate records reflecting our Processing including records of Data Subjects' Consents and procedures for obtaining Consents in accordance with the Council's record keeping guidelines.

These records should include, at a minimum, the name and contact details of the Data Controller and the DPO, clear descriptions of the Personal Data types, Data Subject types, Processing activities, Processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

13.3 TRAINING AND AUDIT

The council are required to ensure all Council Personnel have undergone adequate training to enable them to comply with data privacy laws. We must also regularly test our systems and processes to assess compliance.

You must undergo all mandatory data privacy related training and ensure your team undergo similar mandatory training in accordance with the Council's mandatory training guidelines.

You must regularly review all the systems and processes under your control to ensure they comply with this Privacy Standard and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

13.4 PRIVACY BY DESIGN AND DATA PROTECTION IMPACT ASSESSMENT (DPIA)

The Council are required to implement Privacy by Design measures when Processing Personal Data by implementing appropriate technical and organisational measures (like Pseudonymisation) in an effective manner, to ensure compliance with data privacy principles.

You must assess what Privacy by Design measures can be implemented on all programs/systems/processes that Process Personal Data by taking into account the following:

(a) the state of the art;

(b) the cost of implementation;

(c) the nature, scope, context and purposes of Processing; and

(d) the risks of varying likelihood and severity for rights and freedoms of Data Subjects posed by the Processing.

Data controllers must also conduct DPIAs in respect to high risk Processing.

You should conduct a DPIA (and discuss your findings with the DPO) when implementing major system or business change programs involving the Processing of Personal Data including:

(e) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);

(f) Automated Processing including profiling and ADM;

(g) large scale Processing of Sensitive Data; and

(h) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

(i) a description of the Processing, its purposes and the Data Controller's legitimate interests if appropriate;

(j) an assessment of the necessity and proportionality of the Processing in relation to its purpose;

(k) an assessment of the risk to individuals; and

(l) the risk mitigation measures in place and demonstration of compliance.

You must comply with the Council's guidelines on DPIA and Privacy by Design.

13.5 AUTOMATED PROCESSING (INCLUDING PROFILING) AND AUTOMATED DECISION-MAKING

Generally, ADM is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

If certain types of Sensitive Data are being processed, then grounds (b) or (c) will not be allowed but such Sensitive Data can be Processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

The Council must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

A DPIA must be carried out before any Automated Processing (including profiling) or ADM activities are undertaken.

Where you are involved in any data Processing activity that involves profiling or ADM, you must comply with the Council's guidelines on profiling or ADM if applicable.

13.6 DIRECT MARKETING

The Council are subject to certain rules and privacy laws when marketing to our customers.

For example, a Data Subject's prior consent is required for electronic direct marketing (for example, by email, text or automated calls). The limited exception for existing customers known as "soft opt in" allows organisations to send marketing texts or emails if they have obtained contact details in the course of a sale to that person, they are marketing similar products or services, and they gave the person an opportunity to opt out of marketing when first collecting the details and in every subsequent message.

The right to object to direct marketing must be explicitly offered to the Data Subject in an intelligible manner so that it is clearly distinguishable from other information.

A Data Subject's objection to direct marketing must be promptly honoured. If a customer opts out at any time, their details should be suppressed as soon as possible. Suppression involves retaining just enough information to ensure that marketing preferences are respected in the future.

You must comply with the Council's guidelines on direct marketing to customers.

13.7 SHARING PERSONAL DATA

Generally the Council are not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

You may only share the Personal Data we hold with another employee, agent or representative of the Council if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

You may only share the Personal Data we hold with third parties, such as our service providers if:

(a) they have a need to know the information for the purposes of providing the contracted services;

(b) sharing the Personal Data complies with the Privacy Notice provided to the Data Subject and, if required, the Data Subject's Consent has been obtained;

(c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;

(d) the transfer complies with any applicable cross border transfer restrictions; and

(e) a fully executed written contract that contains GDPR approved third party clauses has been obtained.

You must comply with the Council's guidelines on sharing data with third parties.

14. CHANGES TO THIS PRIVACY STANDARD

The Council reserve the right to change this Privacy Standard at any time without notice to you so please check back regularly to obtain the latest copy of this Privacy Standard.

This Privacy Standard does not override any applicable national data privacy laws and regulations in countries where the Council operates. Certain countries may have localised variances to this Privacy Standard which are available upon request to the DPO.

This page is intentionally left blank

Chorley Council

Data Usage Policy

2018

Version 1.1 February 2018

Table of Contents

INTRODUCTION

Changes in technology have resulted in us communicating and gathering information from our stakeholders via many new methods. The majority of our data gathering is now done so electronically.

The introduction of GDPR in May 2018 also brings changes to the rights of individuals who we hold personal data about.

We need to ensure we communicate certain information to individuals about how their information will be used, stored, how long it will be retained for and the rights they have relating to that data. This needs to be clear and concise; we need to ensure this is worded as simply as possible and delivered to the data subject at the correct time.

Article 13 of the GDPR sets out what information we must provide when we are collecting personal data from a data subject; it specifies we must provide the following information at the point when the data subject provides their personal information:

- Who we are (when acting as Data Controller) and our contact details
- Contact details of our Data Protection Officer
- The purposes of the processing for which personal data are intended, as well as the legal basis for the processing
- If applicable, the legitimate interests
- The recipients or categories of recipients of the personal data, if any
- If we intend to transfer personal data to third countries or international organisations
- For what period the personal data will be stored; or if that's not possible, the criteria used to determine that period
- of their right to request access to held information
- of their right to rectification
- of their right to erasure of personal data (where applicable)
- of their right to restriction of processing (where applicable)
- of their right to data portability
- of their right to withdraw consent (where applicable)
- of their right to lodge a complaint with the supervisory authority (ICO)
- Whether the provision of personal data is a statutory or contractual requirement, whether the Data Subject is obliged to provide the personal data and of possible consequences of failure to provide data
- The existence of any automated decision making. If automated decision making is used, we must provide meaningful information about the logic involved, the significance and envisaged consequences of such processing for the Data Subject

Article 13 also explains that we must notify the data subject if we intend to further process the personal data for a purpose or purposes other than that for which the personal data were originally collected.

Article 14 also sets out requirements when personal data is obtained but is not directly obtained from the data subject. The same information must be provided as detailed above, however, rather than being provided at the point when the data subject provides the information, instead it must be provided:

- within a reasonable period after obtaining the information, at least within one month, having regard to the specific circumstances in which the personal data are processed
- if disclosure to another recipient is envisaged, at the latest when the personal data is first disclosed

- if personal data are to be used for communication with the data subject, at the latest at the time of the first communication with the data subject

For information, Article 4(1) of the GDPR defines personal data as:
'personal data means any information relating to an identified or identifiable nature person ('data subject); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person'
Essentially this is information from which an individual person can be identified.

PURPOSE

The purpose of this policy is to identify appropriate and inappropriate use of data and to ensure Chorley Council meets its requirements of advising data subjects of rights available to them. We must inform individuals:

- how we will process their data
- if their data will be shared
- of the rights they are entitled to
- the required contact details
- how long data will be stored for
- whether submission of personal data is a statutory or contractual requirement
- of any automated decision making take place

POLICY OBJECTIVES

The objective of this policy is to create a set of guidelines that will detail:

- the information we need to provide to individuals when they provide personal information to us, or
- the information we will communicate to individuals when we receive their data via another channel; and
- when and how the information will be communicated

SCOPE

This policy applies to all personal information held by Chorley Council.

POLICY STATEMENT

Chorley Council will ensure that the required information is communicated with data subjects at the correct time.

Where data is gathered directly from the Data Subject, the required information will be provided at point of gathering the data.

Where data is provided by another source or channel, the required information will be communicated with the Data Subject as soon as possible. We will communicate the information within one month of its receipt, wherever possible.

On receipt of personal data, we will advise the Data Subject of:

- Who we are (when we are acting as Data Controller) and our contact details
- Contact details of our Data Protection Officer
- The purposes the information has been requested for; how we intend to process the personal data, as well as the legal basis for the processing
- If applicable, the legitimate interests
- Whether or not the personal data will be shared and if so, who it will be shared with or details of the categories of recipients who it will be shared with
- If we intend to transfer their personal data to countries based outside EU or international organisations
- How long we will store the personal data for; or where this is not possible, the criteria used to determine that period
- their right to request access to held information
- their right to rectification; have errors corrected
- their right to erasure of personal data (where applicable)
- their right to restriction of processing (where applicable)
- their right to data portability
- their right to withdraw consent (where applicable)
- their right to lodge a complaint with the supervisory authority (ICO)
- Whether or not them providing their personal data is a statutory or contractual requirement
- whether the Data Subject is obliged to provide the personal data and of possible consequences of failure to provide data
- The existence of any automated decision making.
- If automated decision making is used, we must provide meaningful information about the logic involved, the significance and envisaged consequences of such processing for the Data Subject

Role	Responsibility	Frequency
All officers (All Directorates)	Ensure they are aware of and understand the wording of the Privacy Notice and digital opt-in arrangements	Ongoing
	Will make their line manager aware, if they become aware of any problems with the Privacy Notice webpage / opt-in function	Ongoing
Line Managers / Team Leaders (All Directorates	Ensure their staff are aware of and understand the Privacy Notice	On-going
	Ensure any problems reported or identified with the Privacy Notice webpage / function are reported to ICT as soon as possible	On-going
Data Controllers (All Directorates)		On-going
		On-going
Data Protection Officer	Is aware of any changes to the GDPR, particularly those which may result in the amendments to the Privacy Notice	On-going
Directors/Heads of Service		
Chief Executive	Overall Officer level responsibility	
Internal Audit	Produce reports following internal audits, with recommendations for improvements in procedures	On-going
	Undertake spot checks as identified	On-going
Policy & Communications		Bi-ennually
	Undertake spot checks as required and identified in the risk assessment	On-going
ICT Team	The Information Manager will have overall responsibility for ensuring online notifications such as Privacy Notices displayed as webpages and digital opt-in arrangements are operational	As required
	To carry out necessary work to ensure webpage based Privacy Notice and digital opt-in arrangements are functioning correctly and remain operational	As required

MONITORING AND REVIEW ARRANGEMENTS

This policy will be reviewed annually (or as required following legislative changes).

DOCUMENT AND VERSION CONTROL

Version	1.1
Author	Ally Lloyd, GDPR Compliance Officer, Chorley Council
Sign off date	
Publication date	

Chorley Council

GENERAL PRIVACY NOTICE

Your personal data – what is it?

"Personal Data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address or address.)Identification can be directly using the data itself by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify staff in the first list then the first list will also be treated as personal data) The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

Who are we?

This privacy notice is provided to you by Chorley Council which is the data controller for your data.

Other data controllers the council works with:

- Lancashire County Council
- Community Groups
- Charities
- Contractors
- Credit reference agencies

We may need to share your personal data we hold with them so that they can carry out their responsibilities to the Council. If we and the other data controllers listed above are processing your data jointly for the same purposes, then the Council and the other data controllers may be "joint data controllers" which means we are all collectively responsible to you and your data. Where each of the parties listed above are processing your data for their own independent purposes then each of us will be independently responsible to you and if you have any questions, wish to exercise any of your rights (see below) or wish to raise a complaint, you should do so directly to the relevant controller

A description of what personal data the Council processes and for what purposes is set out in the Privacy Notice.

The Council will process some or all of the following personal data where necessary to perform its tasks:

- Names, titles, aliases, photographs;
- Contact details such as telephone numbers, addresses, and email addresses;

- Where they are relevant to the services provided by a Council,. Or where you provide them to us, we may process information such as gender, age, marital status, nationality, education, work history, academic/professional qualifications, hobbies, family composition, and dependants;
- Where you pay for activities such as use of a Council Hall, financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers and claim numbers
- The personal data we process may include sensitive or other special categories of personal data such as criminal convictions, racial or ethnic origin, mental and physical health, details of injuries, medical/treatment received, political beliefs, trade union affiliation, genetic data, biometric data, data concerning and sexual life or orientation

How we use sensitive personal data

- We may process sensitive personal data including as appropriate:

- information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work

- Your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation

- In order to comply with legal requirements and obligations to third parties.

These types of data are described in the GDPR as “Special Categories of Data” and require higher levels of protection. We need to have justification for collecting, storing and using this type of personal data.

We may process special categories of personal data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where we need to carry out our legal obligations
- Where it is needed in the public interest

Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else’s interests) and you are not capable of giving your consent, where you have already made the information public.

Do we need your consent to process your sensitive data?

In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will provide you with full details of the personal data that we would like and the reason we need it so that you can carefully consider whether you wish to consent.

The Council will comply with data protections law. This says that the personal data we hold about you must be:

- Used lawfully, fairly and in a transparent way
- Collected only for valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes.
- Relevant to the purposes we have told you about and limited only to those purposes
- Accurate and kept up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

We use your personal data for some or all of the following purposes:

- To deliver public services including to understand your needs to provide the services that you request and to understand what we can do you and inform you of other relevant services
- To confirm your identity to provide some services
- To contact you by post, email, telephone or using social media (e.g. Facebook, Twitter, Whatsapp)
- To help us build up a picture of how we are performing
- To prevent and detect fraud and corruption in the use of public funds and where necessary for the law enforcement functions
- To enable us to meet all legal and statutory obligations and powers including any delegated functions
- To carry out comprehensive safeguarding procedures (including due diligence and complaints handling) in accordance with best safeguarding practice from time to time with the aim of ensuring that all children and adults at risk are provided with safe environments and generally as necessary
- To promote the interests of the Council
- To maintain our own accounts and records
- To seek your views, opinions and comments
- To notify you of changes to our facilities, services, events and staff, councillors and other role holders.
- To send you communications which you have requested and that may be of interest to you
- These may include information about campaigns, appeals, other new projects or initiatives
- To process relevant financial transactions including grants and payments for goods and services supplied to the Council
- To allow the statistical analysis of data so we can plan the provision of services
- Our processing may also include the use of CCTV systems for the prevention and prosecution of crime.

What is the legal basis for processing your personal data

The Council is a public authority and has certain powers and obligations. Most of your personal data is processed for compliance with a legal obligation which includes the discharge of the Council's statutory functions and powers. Sometimes when exercising these powers or duties it is necessary to process personal data of residents or people using the

Council's services. We will always take into account your interests and rights. This privacy notice sets out your rights and the Council's obligations to you.

We may process personal data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract. An example of this would be processing your data in connection with the use of sports facilities, or the acceptance of an allotment garden tenancy.

Sometimes the use of your personal data requires your consent. We will first obtain your consent to that use.

Sharing your personal data

This section provides information about the third parties whom the Council may share your personal data. These third parties have an obligation to put in place appropriate security measures and will be responsible to you directly for the manner in which they process and protect your personal data. It is likely that we need to share your data with some or all of the following (but only where necessary):

- The data controller listed above under the heading "Other data controllers the council works with"
- Our agents, suppliers and contractors. For example. We may ask a commercial provider to publish or distribute newsletters on our behalf or to maintain our database software
- On occasion, other local authorities or not for profit bodies with which we are carrying out joint ventures e.g. in relation to facilities or events for the community

How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example, it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The Council is permitted to retain data in order to defend or pursue claims. In some cases the law imposes a time limit for such claims (for example 3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or purse a claim. In general we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

Your rights and your personal data

You have the following rights with respect to your personal data:

When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. **The right to access personal data we hold on you**

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month

- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. **The right to correct and update the personal data we hold on you**

   If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

   .

3. **The right to have personal data erased**

   If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase their personal data we hold. When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it to comply with a legal obligation.)

4. **The right to object to processing of your personal data or to restrict it to certain purposes only**

   You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. **The right to data portability**

   You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained**

   You can withdraw your consent easily by telephone, email, or by post (see Contact Details below)

7. **The right to lodge a complaint with the Information Commissioner's Office**

You can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.ujk/global/contact-us/email or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measure giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible overseas so on occasion some personal data (for example in a newsletter) may be accessed overseas.

Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing.

Changes to this notice

We keep this Privacy Notice under regular review and will place any updates on this webpage. This Notice was last updated 16th May 2018

Contact Details

Please contact us if you have any questions about this privacy notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Head of Legal, Democratic and HR Services, Chorley Borough Council, Town Hall, Market Street, Chorley, PR7 1DP

Email: contact@chorley.gov.uk

Telephone: 01257 515151

GENERAL PRIVACY NOTICE

For Staff*, Councillors and Role Holders**

*Staff means employees, workers, agency staff, and those retained on a temporary or permanent basis.

**Includes volunteers, contractors, agents and other role holders within the Council including former staff and former councillors. This also includes applicants or candidates for any of these roles.

1. **Your personal data – what is it?**

"Personal Data" is any information about a living individual which allows them to be identified from that data (for example a name, photographs, videos, email address or address.)Identification can be directly using the data itself by combining it with other information which helps to identify a living individual (e.g. a list of staff may contain personnel ID numbers rather than names but if you use a separate list of the ID numbers which give the corresponding names to identify staff in the first list then the first list will also be treated as personal data) The processing of personal data is governed by legislation relating to personal data which applies in the United Kingdom including the General Data Protection Regulation (the "GDPR") and other legislation relating to personal data and rights such as the Human Rights Act.

2. **Who are we?**

This privacy notice is provided to you by Chorley Council which is the data controller for your data.

The Council works together with:

- Other data controllers such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers
- DBS service providers
- Payroll service providers
- Recruitment Agencies
- Credit Reference Agencies

We may need to share personal data we hold with them so that they can carry out their responsibilities to the council and our community. The organisations referred to above will sometimes be "joint data controllers". This means we are all responsible to you for how we process your data where for example tow more data controllers are working together for a joint purpose. If there is no joint purpose or collaboration then the data controllers will be independent and will be individually responsible to you.

3. **The Council will comply with data protection law. This says that the personal data we hold about you must be:**

- Used lawfully, fairly and in a transparent way
- Collected only for a valid purposes that we have clearly explained to you and not used in any way that is incompatible with those purposes
- Relevant to the purposes we have told you about and limited only to those purposes
- Accurate and up to date
- Kept only as long as necessary for the purposes we have told you about
- Kept and destroyed securely including ensuring that appropriate technical and security measures are in place to protect your personal data to protect personal data from loss, misuse, unauthorised access and disclosure.

4. What data do we process?

- Names, titles and aliases, photographs
- Start date/leave date
- Contact details such as telephone numbers, addresses and email addresses
- Where they are relevant to our legal obligations, or where you provide them to us, we may process information such as gender, age, date of birth, marital status, nationality, education/work history, academic/professional qualifications, employment details, hobbies, family composition, and dependants
- Non-financial identifiers such as passport numbers, driving licence numbers, vehicle registration numbers, taxpayer identification numbers, staff identification numbers, tax reference codes and national insurance numbers.
- Financial identifiers such as bank account numbers, payment card numbers, payment/transaction identifiers, policy numbers and claim numbers
- Financial information such as National Insurance Number, pay and pay records, tax code, tax and benefits contributions, expenses clamed
- Other operational personal data created, obtained, or otherwise processed in the course of carrying out our activities, including but not limited to CCTV footage, recordings of telephone conversations, IP addresses, and website visit histories, logs of visitors and log of accidents, injuries and insurance claims.
- Next of kin and emergency contact information
- Recruitment information (including copies of right to work documentation, references and other information included in a CV or cover letter or as part of the application process and referral source (e.g.agency, staff referral)
- Location of employment or workplace
- Other staff data (not covered above) including: level, performance management information, languages and proficiency; licences, certificates, immigration status,; employment status; information for disciplinary and grievance proceedings; and personal biographies
- CCTV footage and other information obtained through electronic means such as swipecard records
- Information about your use of our information and communication systems

Chorley Council

5. **We use your personal data for some or all of the following purposes:-**

- Making a decision about your recruitment or appointment
- Determining the terms on which you work for us
- Checking you are legally entitled to work in the UK
- Paying you and if you are an employee, deducting tax and National Insurance contributions
- Providing any contractual benefits to you
- Liaising with your pension provider
- Administering the contract we have entered into with you
- Management and planning including accounting and auditing
- Conducting performance reviews, managing performance and determining performance requirements
- Making decisions about salary reviews and compensation
- Assessing qualifications for a particular job or task, including decisions about promotions
- Conducting grievance or disciplinary proceedings
- Making decisions about your continued employment or engagement
- Making arrangements for the termination of our working relationship
- Education, training and development requirements
- Dealing with legal disputes involving you including accidents at work
- Ascertaining your fitness to work
- Managing sickness absence
- Complying with health and safety obligations
- To prevent fraud
- To monitor your use of our information and communication systems to ensure compliance with our IT policies
- To ensure network and information security, including preventing unauthorised access to our computer and electronic communications systems and preventing malicious software attrition rates
- Equal Opportunities Monitoring
- To undertake activity consistent with our statutory functions and powers including any delegated functions.
- To maintain our own accounts and records
- To seek your views or comments
- To process a job application
- To administer councillor's interests
- To provide a reference

Our processing may also include the use of CCTV systems for monitoring purposes.

6. Some of the above grounds for processing will overlap and there may be several grounds which justify our use of your personal data.

7. We will only use your personal data when the law allows us to. Most commonly we will use your personal data in the following circumstances:

- Where we need to perform the contract we have entered into with you.
- Where we need to comply with a legal obligation.

8. We may also use your personal data in the following situations, which are likely to be rare:

- Where we need to protect your interests (or someone else's interests)
- Where it is needed in the public interest (or for official purposes)

9. How we use sensitive personal data

9.1 We may process sensitive personal data relating to staff, councillors and role handlers including as appropriate:
- Information about your physical or mental health or condition in order to monitor sick leave and take decisions on your fitness for work
- Your racial or ethnic origin or religious or similar information in order to monitor compliance with equal opportunities legislation
- In order to comply with legal requirements and obligations to third parties

9.2 These types of data are described in the GDPR as "Special Categories of Data" and require higher levels of protection. We need to have further justification for collecting, storing and using this type of personal data.

9.3 We may process special categories of personal data in the following circumstances:

- In limited circumstances, with your explicit written consent
- Where we need to carry out our legal obligations
- Where it is needed to assess your working capacity on health grounds, subject to appropriate confidentiality safeguards

9.4 Less commonly, we may process this type of personal data where it is needed in relation to legal claims or where it is needed to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

10. Do we need your consent to process your sensitive data?

10.1 We do not need your consent if we use your sensitive personal data in accordance with our rights and obligations in the field of employment and social security law

10.2 In limited circumstances, we may approach you for your written consent to allow us to process certain sensitive personal data. If we do so, we will

provide you with full details of the personal data that we would like and the reason we need it, so that you can carefully consider whether you wish to consent.

10.3 You should be aware that it is not a condition of your contract with us that you agree to any request for consent from us

11. Information about criminal convictions

11.1 We may only use personal data relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and provided we do so in line with our data protection policy.

11.2 Less commonly we may use personal data relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interest) and you are not capable of giving your consent, or where you have already made the information public.

11.3 We will only collect personal data about criminal convictions if it is appropriate given the nature of the role and where we are legally able to do so. Where appropriate, we will collect personal data about criminal convictions as part of the recruitment process or we may be notified of such personal data directly by you in the course of you working for us.

12. What is the legal basis for processing your personal data?

12.1 Some of our processing is necessary for compliance with a legal obligation

12.2 We may also process data if it is necessary for the performance of a contract with you, or to take steps to enter into a contract.

12.3 We will also process your data in order to assist you in fulfilling your role in the Council including administrative support or if processing is necessary for compliance with a legal obligation.

13. Sharing your personal data

Your personal data will only be shared with third parties including other data controllers where it is necessary for the performance of the data controllers' tasks or where you first gave us your prior consent. It is likely that we will need to share your data with:

- Our agents, suppliers and contractors. For example we may ask a commercial provider to manage our HR/payroll functions, or to maintain our database software;
- Other persons or organisations operating within the local community
- Other data controllers, such as local authorities, public authorities, central government and agencies such as HMRC and DVLA
- Staff pension providers
- Former and prospective employers

- DBS service suppliers
- Payroll service providers
- Recruitment Agencies
- Credit reference agencies
- Professional Advisors
- Trade Union or employee representatives

14. How long do we keep your personal data?

We will keep some records permanently if we are legally required to do so. We may keep some other records for an extended period of time. For example it is currently best practice to keep financial records for a minimum period of 8 years to support HMRC audits or provide tax information. We may have legal obligations to retain some data in connection with our statutory obligations as a public authority. The Council is permitted to retain data in order to defend or pursue claims. In some cases, the law imposes a time limit for such claims (3 years for personal injury claims or 6 years for contract claims). We will retain some personal data for this purpose as long as we believe it is necessary to be able to defend or pursue a claim. In general we will endeavour to keep data only for as long as we need it. This means that we will delete it when it is no longer needed.

15. Your responsibilities

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

16. Your rights in connection with personal data

16.1 You have the following rights with respect to your personal data:

16.2 When exercising any of the rights listed below, in order to process your request, we may need to verify your identity for your security. In such cases we will need you to respond with proof of your identity before you can exercise these rights.

1. The right to access personal data we hold on you

- At any point you can contact us to request the personal data we hold on you as well as why we have that personal data, who has access to the personal data and where we obtained the personal data from. Once we have received your request we will respond within one month

- There are no fees or charges for the first request but additional requests for the same personal data or requests which are manifestly unfounded or excessive may be subject to an administrative fee.

2. The right to correct and update the personal data we hold on you

If the data we hold on you is out of date, incomplete or incorrect, you can inform us and your data will be updated.

.

3. **The right to have personal data erased**

   If you feel that we should no longer be using your personal data or that we are unlawfully using your personal data, you can request that we erase their personal data we hold. When we receive your request we will confirm whether the personal data has been deleted or the reason why it cannot be deleted (for example because we need it to comply with a legal obligation.)

4. **The right to object to processing of your personal data or to restrict it to certain purposes only**

   You have the right to request that we stop processing your personal data or ask us to restrict processing. Upon receiving the request we will contact you and let you know if we are able to comply or if we have a legal obligation to continue to process your data.

5. **The right to data portability**

   You have the right to request that we transfer some of your data to another controller. We will comply with your request, where it is feasible to do so, within one month of receiving your request.

6. **The right to withdraw your consent to the processing at any time for any processing of data to which consent was obtained**

   You can withdraw your consent easily by telephone, email, or by post (see Contact Details below)

7. **The right to lodge a complaint with the Information Commissioner's Office**

   You can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.ujk/global/contact-us/email or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF

17. Transfer of Data Abroad

Any personal data transferred to countries or territories outside the European Economic Area ("EEA") will only be placed on systems complying with measure giving equivalent protection of personal rights either through international agreements or contracts approved by the European Union. Our website is also accessible overseas so on occasion some personal data (for example in a newsletter) may be accessed overseas.

18. Further processing

If we wish to use your personal data for a new purpose, not covered by this Privacy Notice, then we will provide you with a new notice explaining this new use prior to commencing the processing and setting out the relevant purposes and processing conditions. Where and whenever necessary, we will seek your prior consent to the new processing, if we start to use your personal data for a purpose not mentioned in this notice.

Changes to this notice

We keep this Privacy Notice under regular review and will place any updates on this webpage [add url]. This Notice was last updated May 2018

Contact Details

Please contact us if you have any questions about this privacy notice or the personal data we hold about you or to exercise all relevant rights, queries or complaints at:

The Data Controller, Head of Legal, Democratic and HR Services, Chorley Borough Council, Town Hall, Market Street, Chorley, PR7 1DP

Email: contact@chorley.gov.uk

Telephone: 01257 515151

You can contact the Information Commissioner's Office on 0303 123 1113 or via email https://ico.org.uk/global/contact-us/email or at the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Report of	Meeting	Date
Director of Policy and Governance (Introduced by the Executive Member for Economic Development and Public Service Reform)	Full Council	15/05/2018

LCC TRANSFORMATION FUND 18/19 AND 19/20 – REQUEST FOR ADDITIONAL FUNDING

PURPOSE OF REPORT

1. The purpose of this report is to seek approval for additional funding of up to £58,000 to support the LCC Transformation fund in 18/19 and £43,000 in 19/20 to support the provision of future bus services, jointly funded by LCC and the Council. Total additional expenditure for 2018/19 and 2019/20 is £100,000.

2. The report will also seek to delegate approval for the expenditure of funding towards the subsidised bus services to be undertaken by the Leader, and issuing of tender contract through LCC. This will be undertaken by an EMD in late Summer 2018.

RECOMMENDATION(S)

3. To increase the 2018/19 LCC Transformation Fund budget by £58,000, to a total of £158,000 to subsidised bus services in the borough.

4. That the awarding of the Tender for the proposed 357 service, be awarded by the Executive Member for Economic Development and Public Service Reform via an EMD once a cost tender exercise has been undertaken by LCC.

EXECUTIVE SUMMARY OF REPORT

5. This report provides a summary of the current financial position regarding the provision of Council-funded bus services within Chorley. It also outlines the proposals to move to a tendered solution, to provide a more sustainable suite of subsidised bus provision, funded by the Council, and LCC within the borough.

6. Chorley Council's current bus subsidy 2017/18 costs approximately £225,000 per annum. The majority of routes are solely funded by the Council, with 30% funding from LCC towards the 109B/4A services. Chorley Council subsidises 70% of this bus route to LCC, who have tendered the contract.

7. Our overall subsidy contribution funds four current routes are outlined below (table included in paragraph 9). The current cost arrangements are expensive, and are not sustainable. In order to deliver more sustainable bus services, and increase LCC funding into the subsidised routes, the existing routes have been re-designed into three routes combining the majority of the current 7C and 6/6Aprovision into a new 357 service. Details of these routes are outlined below at the table included in paragraph 10.

8. The current bus services, supported by the Council are:

Bus no	Route	Annual Cost 2017/18 (approx.)	Current Operator
109 B (formerly 109A route subsidised by LCC)	Chorley – Astley Village **Evening and weekend**	Chorley Council pay 70% to LCC (£39,897) LCC pay remaining 30%	Stagecoach
4A (formerly 24A previously LCC)	Chorley-Wheelton-Brinscall- Abbey Village **Evening and weekend**		
7C (previously commercial operator)	Chorley Central service (Chorley bus station, Pall Mall, Harrison Road to Carr Lane, Red Bank Melrose Way)	£98,397	Stagecoach
6/6A (previously LCC)	Chorley-Coppull	£86,266	Holmeswood
TOTAL FUNDED BY COUNCIL		**£224,560**	

9. The future services proposed to be delivered are:

Service	Description of service	Cost (approximate)
Continuation of 109B/4A	Evening and weekend service, Chorley to Astley Village. Continuing the current service provision	£62,000
NEW 357	Monday to Saturday service. A combination of the majority of the existing 7C/6A services.	£77,000
	Total Proposed Cost	**£139,000**

10. The costs are approximate, as no formal tender process has yet been undertaken by LCC. However, they are confident upon their estimations, as they are based upon similar service provision, and are within their procurement guidelines.

11. The new route (357), will be tendered by LCC, and all future routes will be funded by Chorley Council and LCC. The cost of services outlined above will be approximately £139,000 per annum, with Chorley Council's contribution being £83,400 (60% of the total cost) and LCC's contribution being £55,600 (40% of the future cost). This significantly reduces the cost of bus subsidy to the Council from £225,000 per annum, to approximately £83,400 per annum.

12. The option exists for the Council to serve notice on the services. This requires a 12 week notice period for the services to be terminated if a decision is made to no longer subsidise bus services in the future.

13. Future approvals of funding associated with the bus subsidy, will be undertaken as part of the standard budget-setting process for 2019/20.

Confidential report Please bold as appropriate	Yes	**No**

CORPORATE PRIORITIES

14. This report relates to the following Strategic Objectives:

Involving residents in improving their local area and equality of access for all	✓	A strong local economy	
Clean, safe and healthy homes and communities		An ambitious council that does more to meet the needs of residents and the local area	✓

BACKGROUND

15. Lancashire County Council (LCC) is responsible for providing public transport services across the county. At the end of 2015/16, LCC reduced their funding to subsidised bus services across Lancashire for the 2016/17 financial year. This had an impact upon a number of bus services within Chorley, and the decision was taken by the Council, to provide a subsidy for the 6/6A and 109B/4A routes.

16. The current 6/6A service provides a route from the town centre to Coppull and Gillibrand, and provides coverage within the following wards: Chorley South East, Chorley North West, Chorley South West and Coppull.

17. The 109B/4A provides an evening and weekend service from Chorley town centre to Astley Village, and provides a service within the following wards: Chorley North West, Astley and Buckshaw, Chorley South East, Chorley East, Chorley North East, Pennine, Wheelton and Withnell and Brindle and Hoghton.

18. In February 2017, the commercial operator, Stagecoach, withdrew the 7 (now the 7C) for operations, citing that it was no longer commercially viable for them to operate. A decision was made to fund the provision of this service, and this has been ongoing since February 2017.

19. The 7C route covers Chorley town centre, Pall Mall, Harrison Road to Carr Lane, Red Bank and Melrose Way, and provides a service within the ward of Chorley South East.

20. Expenditure to date on these services, by the Council in previous years has been as follows:-

Service	2016/17	2017/18	
109B/4A (Council contribution)	29,045	39,897	
6/6A	84,351	86,266	
7C	18,643	98,297	
TOTAL	**132,038**	**224,559**	**356,597**

21. LCC currently part-fund the 109B/4A at 30% at a cost of approximately £18,600 per annum. The future arrangements would see the LCC contribution to the 109B/4A increase to 40% at £24,800, and LCC would part fund 357 route at £30,800. A total annual contribution of £55,600 will be provided by LCC towards the future bus provision.

22. Without funding from the Council, the above services would not operate, and coverage would be lost.

CURRENT POSTION

23. Over recent months, a significant amount of work has taken place between both Chorley Council and Lancashire County Council to seek a more sustainable approach to the provision of these routes within Chorley. This has considered the following:-

- The current coverage provided by existing bus routes, and their proximity to other commercial services
- The commercial viability of service provision, designing a new route that would provide fare income, and offset some of the costs of subsidy
- The required coverage to be provided by the route, to meet the statutory and desired provision
- The logistics of re-designing the above, into a route, capable of being delivered within a 60 minute period, by one bus (as is a requirement of route design)
- Any changes that have occurred to bus service provision within Chorley, since April 2017.
- Consideration of the existing subsidised bus route, their usage and whether this provision should continue within the context of the current Lancashire bud network.
- Amendments made to an existing commercial route that served Harpers Lane/Eaves lane, in order to address overcrowding on the former service (December 2017).

24. The future bus routes should not impact negatively upon existing commercial routes, or duplicate any existing service provision, as this conflicts with Bus Tender Regulations. Additionally, the Council and LCC would not wish to design a bus route, that reduces the commercial viability of existing routes within the borough, as this could see these services being withdrawn in the future.

FUTURE PROPOSALS

25. A proposed new service (357) has been designed, applying the principles outlined above, that will replace the majority of the existing 7C and the 6/6A service, into one new route. It is proposed that the current 109B/4A evening and weekend service will continue without amendment.

26. The proposed 357 route will provide coverage from the town centre through Chorley South East, Chorley North West and Chorley South West and will be a tendered service, as opposed to an interim-funded option.

27. The current subsidy arrangements cost are high, and are not sustainable. Moving to a tendered solution would reduce the cost significantly, and be part-funded (40%) by LCC, who are supportive of the new route.

28. LCC will be the tendering authority for the new 357 and will continue to manage the continuation of the 109B/4A services, and Chorley Council will provide funding to support this. A cost breakdown is provided below, that highlights the cost of extending the current subsidy arrangements until 1 October 2018, at the latest.

29. Therefore, as the initial 12 month tender will span both the 18/19 and 19/20 financial year, approval is sought to support the current subsidy, and new tendered arrangements until 30 September 2019.

PROCUREMENT PROCESS AND TIMESCALES

30. A period of time is required, to allow LCC to undertake a cost tender exercise for the new route, in addition to a 12 week notice period to allow existing routes to cease, prior to the new route tender to commence.

31. Taking into account the timescales above, the new tendered service contract could be awarded from September/October 2018. Following Council approval, LCC will undertake a cost tender exercise for the new service.

32. Should the new service be tendered in September/October 2018, for a 12 month period, continuation of the current subsidy arrangements will be required until that period, that will allow for the notice period and return of tenders. The implication of this is that insufficient allocation exists within the LCC Transformation Budget for bus services in 2018/19, and no allocation has yet been confirmed for the 2019/20 financial year. Funding is therefore sought to enable the Council and LCC to undertake the necessary tender, procurement and notice period.

33. LCC have awarded their current bus contracts until the end of March 2021, and in order to obtain the most cost effective tender for the new route, a minimum of 12 months would be required. Therefore, additional funding within the LCC Transformation Fund is sought to support the current arrangements until the awarding of a tender, and £42,000 funding for 19/20, to support the award of a 12 month contract (357) and continuation of an existing contract (109B/4A) – 6 months of which would fall within the 19/20 financial year. This would cover the period of 1 October 2018-30 September 2019 as a minimum.

COST BREAKDOWN

34. The total cost of subsiding bus provision in 2018/19 will be approximately £116,000 for the initial six months of the financial year, plus approximately £42,000 for the six months subsidy at the annual rate of £83,400. This brings the total budget requirement to £158,000 for

2018/19, and £42,000 for 2019/20 The revised service provision beyond 1 October 2018, will be £139,000, funded by LCC (40%) £ 55,600 and Chorley Council (60%) £83,400.

35. It must be noted that all costs are approximate and are subject to the completion of relevant tender exercises and passenger numbers using the services across the period.

36. An approach has been made to LCC to seek additional funding, above their allocation of £55,600, to support the current arrangements, prior to tendering a new contract by October 2018. At the time of writing this report, the outcome of this request is not known.

37. The total funding available in the LCC transition fund for 2018/19 is £100,000, leaving a shortfall of £58,000 in 2018/19 and available resources of £43,000 in 2019/20, to allow a 12 month contract to be tendered with an operator from 1 October 2018.

Service	2018/19 costs	19/20 Funding required – to 30 September 2019 (based upon 6 months)
7C	£50,000	£42,000
109B/4A	£21,000	
6/6A	£45,000	
Cost of new arrangements 1 Oct -31 March 19	£42,000	
TOTAL (A)	**£158,000**	**£42,000**
LCC Transformation Fund 2018/19 and 2019/20 (B)	£100,000	£85,000
(Shortfall)/Resources Available (-B-A)	**(£58,000)**	**£43,000**

IMPLICATIONS OF REPORT

38. This report has implications in the following areas and the relevant Directors' comments are included:

Finance	✓	Customer Services	
Human Resources		Equality and Diversity	
Legal		Integrated Impact Assessment required?	
No significant implications in this area		Policy and Communications	

COMMENTS OF THE STATUTORY FINANCE OFFICER

39. The financial implications of extending the subsidised bus service is outlined in the report. A request for revenue resources of £58k must be made to Full Council to provide the necessary budget to deliver the services in 2018/19. If approved, the £58k will come from underspends identified in 2018/19 and this will factored into the first budget monitoring report of 2018/19.

COMMENTS OF THE MONITORING OFFICER

40. The routes listed, except for the 7C, have all been tendered. The Council are entitled to rely on the tender exercise undertaken by LCC to ensure that the services are providing value

for money in relation to cost. The costs incurred to support the 7C, which is a non tendered route are below the EU threshold and do not form part of state aid although it is understood that the provider successfully tendered for similar routes at similar day rates. Members can take comfort that the market has been tested.

REBECCA HUDDLESTON
DIRECTOR OF POLICY AND GOVERNANCE

There are no background papers to this report.

Report Author	Ext	Date	Doc ID
Catherine Hudspith	5248	25/4/18	LCC Transformation Fund – additional budget request

This page is intentionally left blank