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	