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.