



Charnwood



Data Protection Policy

Version: 1.5

Issue Date: January 2019

Status: Final Document

Prepared by: Data Protection and Information Security Officer

Published Date: October 2023

Contents

Policy Governance	2
Review and Revision	2
1..... BACKGROUND	5
What is Personal Data?	5
1.1 Introduction	5
1.2 Aims of the policy	5
1.3 Applicability	5
1.4 Scope	6
1.5 Review and Maintenance	6
1.6 Need for the Policy	6
1.7 Legal Requirements	7
1.8 Policy Statement	7
1.9 Objectives	7
2..... Responsibilities	8
2.1 SIRO	8
2.2 Data Protection Officer	8
2.3 Directors and Heads of Service	9
3..... THE PRINCIPLES	9
3.1 Data Protection Principles	10
3.2 Transfer of data outside the EU	11
3.3 Special Category Data	12
4..... RIGHTS AND REQUESTS	12
4.1 Right to be informed	12
4.2 The other rights	13
4.3 Exemptions	13
4.4 Requests for prevention / detection of crime or fraud investigations	14
4.5 CCTV requests	14
5..... INFORMATION SECURITY	14
5.1 Officer responsibility	14
5.2 Data breaches	15
5.3 Data Protection Impact Assessment	15
5.4 Information Sharing	16
6..... MARKETING	16
6.1 Use of personal data in marketing	17
7..... COMPLIANCE WITH THE LEGISLATION	17
7.1 Elected Members	18
8..... COMPLAINTS	18

I BACKGROUND

Both the General Data Protection Regulation and Data Protection Act 2018 came into force in May 2018 and brought with it enhanced rights for people whose personal data is processed by organisations.

What is Personal Data?

The GDPR Article 4 defines Personal Data as:

'personal data' means any information relating to an identified or identifiable natural 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;'

Personal data can be factual (for example, a name, address or date of birth) or it can be an opinion about that person, their actions and behaviour.

I.1 Introduction

Information and personal data are major assets that the Council has a responsibility to protect and where required by law, to publish. They take many forms and include information and data stored on computers, transmitted across networks, printed out or written on paper, sent by fax, stored on tapes, disks or other electronic media and spoken in conversation or over the telephone.

I.2 Aims of the policy

This Policy provides a framework for the management and protection of personal data held by the Council and to ensure all legal obligations on the Council are met including confidentiality of information relating to personal privacy and security.

I.3 Applicability

This policy applies to all personal data held by the Council. Personal data can take many forms and includes, but is not limited to, the following:

- Hard copy data printed or written on paper.
- Data stored electronically.
- Communications sent by post / courier or using electronic means.
- Stored tape or video.
- Recordings.
- Photographs.

I.4 Scope

The policy applies to all:

- Information and personal data held by the Council whatever format in which it is held;
- Locations from which Council systems are accessed (including home use or other remote use). Where there are links to enable partner organisations to access Council information, prior assurance must be obtained that information security risks have been identified and suitably controlled;
- All staff, agency workers, contractors and volunteers processing the Council's data.

I.5 Review and Maintenance

This policy will replace any previous Data Protection Policy.

This policy is agreed and distributed for use across the Council.

It will be reviewed annually by the Senior Information Risk Officer and Data Protection and Information Security Officer.

I.6 Need for the Policy

The information and personal data stored in the Council's manual and electronic information systems represent an extremely valuable asset on which is placed an ever-increasing reliance for the effective delivery of services. The value of and our reliance on our information makes it necessary to ensure that:

- All systems, manual or electronic, that create, store, archive or dispose of information or personal data are developed, operated, used and maintained in a safe and secure fashion. An up to date Information Asset Register will be maintained.
- The public and all users of the Council's information systems are confident of the confidentiality and accuracy of the information and personal data used.
- All legislative and regulatory requirements are met.
- All transmission and essential sharing of information with partners, be that in manual or electronic format, is properly authorised and effected within agreed sharing protocols.

Failure to comply with the requirements of the Data Protection legislation can result in the regulator imposing a fine. The maximum fine the council may face is £17 million.

1.7 Legal Requirements

The Council is obliged to comply with all relevant legislation, and particularly in this context, the Data Protection Act 2018, incorporating the General Data Protection Regulation.

This requirement to comply is also devolved to Elected Members who may be held personally accountable for any breaches of personal data security for which they may be held responsible.

1.8 Policy Statement

This policy aims to assist staff, contractors and volunteers with meeting their statutory and other obligations which covers the issues of Data Protection. It is not a substitute for the Law and if any of the above persons are unsure about its application or interpretation, they should refer the matter to the Data Protection and Information Security Officer.

1.9 Objectives

The policy is intended to establish and maintain the security and confidentiality of personal data, and provide a framework for maintaining the normal business activities of the Council by:

- Creating and maintaining within the organisation a level of awareness of the need for Data Protection as an integral part of the day to day business;
- Ensuring that all data users are aware of and fully comply with the relevant legislation as described in policies and fully understand their own responsibilities;
- Ensuring that all data users are aware of the rights of data subjects in accessing and correcting their personal data under the Data Protection Act 2018;
- Protecting sensitive personal data from unauthorised disclosure;
- Safeguarding the accuracy of information;
- Protecting against unauthorised modification of information
- Storing, archiving and disposing of sensitive and confidential information in an appropriate manner;
- Lawful use or sharing of Council information.

The Council will achieve this by ensuring that:

- Confidentiality of personal data and exempt information is assured;
- Regulatory and legislative requirements are met;
- All transmission and essential sharing of information internally or with partners, in manual or electronic format, is properly authorised and effected within agreed sharing protocols.
- Annual Data Protection training is provided;
- All losses of personal data, actual or suspected, are reported, investigated and any resulting necessary actions taken;
- Standards, guidance and procedures are produced to support this policy.

2 Responsibilities

All employees and Elected Members have responsibilities under the Data Protection Legislation – to adhere to the legislation and this policy; however some officers have some specific responsibilities.

Employee's responsibilities in relation to data protection are set out in:

- Their contract
- This policy
- The Council's constitution
- Council induction
- Annual training

2.1 SIRO

The Strategic Director of Corporate Services is the Senior Information Risk Owner (SIRO) and has overall responsibility for Information Governance & Risk within the Council.

2.2 Data Protection Officer

The Data Protection and Information Security Officer is responsible for:

- Undertaking the mandatory role of Data Protection Officer as defined in the General Data Protection Regulation and the relevant tasks defined within the Regulation
- Developing, implementing and maintaining the corporate Data Protection and Freedom of Information policies, procedures and standards that underpin the effective and efficient creation, management, dissemination and use of personal data;

-
- Provision of Data Protection and Freedom of Information support and advice to Officers;
 - The production, review and maintenance of Data Protection and Freedom of Information policies and their communication to the whole Council;
 - Provision of professional guidance on all matters relating to Data Protection and Freedom of Information;
 - Oversight management and recording of all information data protection breaches and suspected breach investigation;
 - Provision of annual Data Protection Awareness online training module;
 - Management of all information requests under the Data Protection Act 2018, Freedom of Information Act 2000 and Environmental Information Regulations 2004, and any subsequent appeals and complaints to the Information Commissioner;
 - Recording of information sharing agreements;
 - Annual review of Data Protection documents including the Record of Processing Activity and Privacy Notice.

2.3 Directors and Heads of Service

All Directors and Heads of Service will implement this policy within their business areas.

Additionally, they will specifically ensure that:

- All current and future users of Council information are instructed in their data protection responsibilities and have access to and have read the Data Protection Policy and guidance.
- Authorised users of computer systems/media are trained in their use and comply with policy and procedural controls to protect personal data.
- Determine which individuals are given authority to access specific information systems. The level of access to specific systems which contain personal data should be on a job function need, irrespective of status.
- Any breach of this policy, real or suspected, is reported as required in the Data Breach Reporting procedure.
- Any breach investigation is undertaken as a priority and resources are committed to any investigation in order to conclude the investigation in a timely manner.

3 THE PRINCIPLES

All organisations that decide how, why and what 'personal data' is processed are data controllers and are required to pay the appropriate fee to the Information

Commissioner as defined in the Data Protection (Charges and Information) Regulations 2018. Democratic Services ensure that this is completed annually for the Council.

The Council will adopt a “best practice” approach at all times based on the Information Commissioner’ guidelines, and, where appropriate, professional codes of practice.

3.1 Data Protection Principles

All data controllers and processors must observe the Data Protection principles which govern the manner in which data is collected, held and processed. The Council is committed to ensuring that all information held is necessary, used fairly and responsibly and in compliance with the principles as follows:

1. **Processed lawfully, fairly and in a transparent manner**

Information will only be held where it is justified to do so and processing may be carried out where one of the following conditions has been met, namely where:-

(a) Consent: the individual has given clear consent for you to process their personal data for a specific purpose. Services must record that consent has been gained.

(b) Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.

(c) Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations).

(d) Vital interests: the processing is necessary to protect someone’s life.

(e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

(f) Legitimate interests (This condition cannot be used by a Council when carrying out their official functions): the processing is necessary for your legitimate interests or the legitimate interests of a third party unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests.

2. Processed only for specified, explicit and legitimate purposes

The Council is one data controller. Personal data held by the Council can be used within the Council as permitted by the Council's Privacy Notice to carry out the functions of the Council.

This however must be on a 'need to know' basis and appropriate security and access controls implemented where necessary so only staff that need access to the personal data are allowed it.

3. Adequate, relevant and limited to what is necessary

The Council will only hold the minimum personal information necessary to enable it to perform its functions.

4. Accurate and kept up-to-date

All efforts will be made to ensure that information is periodically assessed for accuracy; and is kept up to date.

5. Processed for no longer than is necessary for the purpose(s)

Information must be destroyed securely once it is no longer required and kept in line with the Council's retention and disposal schedule.

6. Protected by appropriate and organisational measures

Staff must refer to the relevant ICS Information Security Policies.

All staff must undergo mandatory annual data protection training.

3.2 Transfer of data outside the EU

Transfer of personal data to non-EU member states must show the necessary organisational and technical measures have been put in place to protect data.

The types of suitable measures include:

- A European Commission Adequacy Decision for the relevant country (the current list of countries is available on the EC website)
- A legally binding and enforceable instrument between public authorities or bodies
- Binding corporate rules
- Standard data protection clauses adopted by the Commission
- Certification under a supervisory authority approved certification mechanism

3.3 Special Category Data

There are additional requirements placed upon the data controller where the holding of 'special category personal data' is concerned. The definition of 'special category personal data' is data in respect of the following: -

- Racial or ethnic origin
- Political opinion
- Religious belief
- Union membership
- Physical/mental health
- Sexual life
- Biometric (for ID purposes)
- Genetic

If disclosing special category personal data (even if required to do so by law), consent of the data subject must be obtained unless a specific exemption applies.

Additionally, if special category personal data is held, security measures for holding such data will need to be considerably higher than that for other service areas holding less sensitive data.

4 RIGHTS AND REQUESTS

All data Subjects have certain rights over their personal data under Data Protection Legislation. These are:

- Right to be Informed
- Right to Access (Subject Access Request)
- Right to Rectification
- Right to Erasure (Right to be Forgotten)
- Right to Object
- Right to Object to Automated Decision-making
- Right to Restriction
- Right to Data Portability

4.1 Right to be informed

Data subjects have the right to know what the Council will use their personal data for. This is called a Privacy Notice, which is published on the Council's website - www.charnwood.gov.uk/privacynotice. The notice should be added to (or sign posted from) all Council forms, including e-forms, where personal data is collected.

The Council must make reasonable efforts to communicate Privacy Notices where necessary to service users with additional needs e.g. but not limited to, translation services, easy read versions, given verbally, posters, leaflets etc.

4.2 The other rights

The procedure for dealing with rights requests is contained in the Data Protection Rights procedure which is available on the Council's Intranet or by request.

If a rights request is received, it should be sent in the first instance, without delay, to the Data Protection and Information Security Officer -
Tel. 01509 634711, Email: foi@charnwood.gov.uk

There is no charge for any of these requests.

The Council has one month in which to respond to rights requests.

The Data Protection and Information Security Officer will consult and request information from the relevant service area/s. Decisions about exemptions to providing information, or to refuse a right, will be made by the Data Protection and Information Security Officer.

4.3 Exemptions

The rights of data subjects are subject to certain statutory exemptions. The Council will disclose personal information, without the data subject's consent in accordance with the GDPR/Data Protection Act 2018. This includes but is not limited to:

- On production of a court order for disclosure of that specific information
- Where the purpose of disclosure is to enable the Authority to assess or collect any tax or duty or any imposition of a similar nature
- Where the purpose of disclosure would be to prevent or detect a crime, apprehend or prosecute offenders
- By order of the Secretary of State
- Where we are obliged by any law to disclose information
- Where information is required for research purposes providing such data is general and does not cause damage or distress to the data subject
- Where disclosure would be to safeguard national security

4.4 Requests for prevention / detection of crime or fraud investigations

The Council often receives ad hoc requests from the police or other authorities, which seek personal information in relation to a particular resident or address in the Borough. These requests should clearly set out what information is sought, why it is required and under what section / exemption of the Data Protection Act their request sits.

Requests should be made in writing, unless it is an emergency. Written requests should be sent to the Data Protection and Information Security Officer.

Police officers should submit such requests on their own form, countersigned by their superior officer.

If any Council staff member is in doubt about releasing information for such requests in an emergency, they should contact the Customer Experience Team immediately for advice.

4.5 CCTV requests

Members of the public can make requests to view CCTV footage which contains images of them, as this is classed as their personal data.

The CCTV team manage these requests, so any requests should be forwarded as soon as possible. Alternatively the data subject can complete the online CCTV request form.

5 INFORMATION SECURITY

The information the Council holds must be kept secure. This is achieved through technical and organisational measures, along with employees understanding their obligations under Data Protection Legislation.

5.1 Officer responsibility

All officers are required to undergo annual Data Protection refresher training, comply with this policy, and with all other information security policies including the Internet and Email Acceptable Usage Policy.

Electronically held personal data should be stored in secure Council IT systems. Where it is necessary to hold personal data locally, it should only be stored on encrypted Council devices. Hard copy personal data must be kept secure, such as in locked filing cabinets, with access restricted to only those employees who have a valid work purpose.

Employees should not take home any manual or computerised files containing personal data. Secure home working access should instead be used.

Failure to adhere to this policy may result in disciplinary action being taken against an officer. If an officer is found to have contravened Data Protection legislation deliberately or through negligence, they may face a criminal investigation and Court Proceedings.

5.2 Data breaches

A data breach is defined as a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data.

This includes breaches that are the result of both accidental and deliberate causes. It also means that a breach is more than just about losing personal data.

Personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

The Council is required to keep a central record of all data breaches, and to report serious breaches to the Information Commissioner's Office (ICO) within 72 hours.

If you become aware of any data breach, you must inform the Data Protection and Information Security Officer without delay.

Further information regarding what to do in the event of a data breach can be found in the Personal Data Breach Reporting Procedure, which is available on the intranet.

5.3 Data Protection Impact Assessment

A Data Protection Impact Assessment (DPIA) is a process to help identify and minimise the data protection risks of a project.

Managers must submit a Data Protection Impact Assessment (DPIA) to the Data Protection and Information Security Officer for all new projects,

procurement, commissioning or services they undertake at the start of any such proceeding.

A DPIA template is available on the intranet.

The Data Protection Officer will assess any final DPIA submission and if he or she feels it meets the necessary ICO criteria, will submit the DPIA to the ICO for consultation as per the ICO's guidance.

5.4 Information Sharing

The Council regularly needs to share personal data with our contractors or partners.

Where sharing is required, the Council requires its partners and agents through contractual terms, partnership agreements or information sharing agreements to comply with the law.

Managers responsible for procurement of services must ensure that data protection impact assessments are carried out, that potential bidders are (and can demonstrate) compliant with data protection requirements, including having relevant and adequate Data Protection policies in place and the necessary Data Processing Agreements are put in place when contracts are awarded. This includes ensuring audit provisions exist in any contract, to enable the Council to critically appraise a Contractor's performance against the Data Protection Principles and enable secure and fast recovery of information if the Contractor's performance slips.

Managers responsible for services which share personal data with outside partners and agencies on a regular, organised basis must ensure that a written Information Sharing Agreement is in place.

All Information Sharing Agreements must be agreed by the Data Protection and Information Security Officer, who will record a copy centrally for monitoring purposes.

6 MARKETING

If the Council uses personal data for the purpose of marketing, this must be done in compliance with the Privacy and Electronic Communications Regulations (PECR).

6.1 Use of personal data in marketing

Personal Data collected by the Council will only be used for marketing purposes where customers have been told this will happen and where customers have explicitly opted-in (consented) to receive such information. Services are also required to keep evidence of consent.

All emails sent to customers for marketing purposes will include a 'how to opt-out' message.

Mailing lists must not be used for any other purpose, or to communicate information unrelated to the original purpose of the mailing list.

7 COMPLIANCE WITH THE LEGISLATION

The Council recognises the need to make the contents of this Policy known and ensure compliance by every employee.

Data Protection awareness will be included in the induction process. Mandatory training updates for staff will also be provided annually. The Data Protection and Information Security Officer will notify staff of changes to Data Protection legislation, how these changes will affect them, when they will occur and what is needed to stay within the law.

The Council also recognises the need to make their policies known and accessible to the public. This policy will be published on the Council's website.

The Council expects all employees to comply fully with this policy, the Data Protection principles, other information legislation and the Council's procedures. Disciplinary action may be taken against any Council employee who breach any instructions contained in or following from this policy.

Individual employees are affected in the same way as the Council as a whole. Anyone contravening the GDPR / Data Protection Act 2018 could be held personally liable and face court proceedings for certain offences which may result in a fine and / or a criminal record.

The Data Protection and Information Security Officer will provide quarterly reports on personal data breaches to the Risk Management Group (CMT).

7.1 Elected Members

On the 1 April 2019, Councillors became exempt from having to pay the Information Commissioner's Data Protection fee where they act as a data controller solely for the purpose of their elected duties. (see [Data Protection \(Charges and Information\) \(Amendment\) Regulations 2019](#) for full details)

However, Councillors must still ensure that Data Protection legislation and policies are complied with, whatever role they may exercise. If the Member is in any doubt, they should contact the Data Protection and Information Security Officer for clarification.

All Councillors will be offered training in Data Protection annually.

8 COMPLAINTS

Complaints relating to any information access request or data protection matter should be made in writing and addressed to:



Data Protection and Information Security Officer
Charnwood Borough Council
Southfields
Southfields Road
Loughborough
LE11 2TR

Data Subjects also have the right to complain to the Supervisory body, which in England is the Information Commissioner.

The ICO can be contacted in writing to:
The Office of the Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Alternatively, please view their website for further information – www.ico.org.uk

Signed for and on behalf of Charnwood Borough Council

Contact Name of Authorised Signatory	 SIMON JAMESON
Role in organisation	STRATEGIC PROTECTION WORK SERVICES
Signature	
Date	17 JAN 2020.