APPENDIX 3

Data Protection Policy

Document Control	
Organisation:	Gateshead Council
Document Name:	Data Protection Policy
Purpose:	Compliance with the UK GDPR and DPA 2018 for processing of personal data
Author:	DPO Team
Published version:	
Date published:	
Date of next review:	2 years from latest version published or sooner should changes to internal processes or legislation occur

Revision / Version History			
Date	**Version**	**Author**	**Comments**
28/06/2022	0.1 DRAFT	DPO Team	DRAFT document for discussion
28/09/2022	0.2 DRAFT	DPO Team (HH)	2nd DRAFT
29/09/2022.	0.3 DRAFT	DPO Team (HH)	3rd DRAFT
28/02/2023	0.4 DRAFT	DPO Team (HH)	Amendments made after consultation
14/04/2023	0.5	DPO (ASM)	Final version for approval

Consultees to this policy	
Title:	DPO, SIRO, Service Director – IT, Cyber Security Group, Corporate Data Protection Group, SMG Services & Performance, CMT

Document Approvals	
This policy is required to be approved by:	Cabinet / Council

Distribution This policy and subsequent revisions will be distributed as follows:	
To	**Method**
All staff	Article published alerting staff of the publication of the updated policies and policies published on the Council intranet.

Contents

Introduction

The UK General Data Protection Regulation ("the GDPR") and the Data Protection Act 2018 (DPA) set out the requirements for public authorities when handling personal information.

The GDPR sets standards and rules and places obligations on those who process personal information while giving rights to those who are the subject of the data. Personal information covers both facts and opinions about the individuals. The rules and procedures cover the collection and use of the data; the quality and security of the data; and the rights of individuals regarding data about themselves.

Gateshead Council ('the Council') is a data controller as it collects and uses information about people to carry out its functions. In some cases, the Council is required by law to collect and use information to comply with central government requirements.

The Council will process personal data relating to local residents, service users, customers, current, past and prospective employees, clients and suppliers in accordance with the requirements of the GDPR, DPA, common law duty of confidentiality and other relevant legislation.

Failure to adhere to this policy may result in disciplinary action for individuals, and enforcement action, financial loss and/or reputational damage to the Council.

Purpose

This policy sets out the Council's approach to complying with the GDPR, DPA and other laws that regulate how personal data is managed. It provides a framework to meet the requirements for data controllers under the legislation and an overview of the main obligations for officers and Members in dealing with personal information.

Scope

Data protection is part of the overarching Information Governance Framework, which describes how personal, confidential and corporate information is managed by the Council. This policy covers all personal data for which the Council is the data controller. When the Council acts as a data processor this policy must be referred to in conjunction with the relevant contract and/or data sharing agreement.

This policy applies to all staff and contractors at the Council. This includes students, temporary, casual, agency staff, volunteers, suppliers and data processors working for or on behalf of the Council.

This policy applies to all personal data collected, created or held by the council, in whatever format (for example paper, electronic, email, microfiche, film, video and audio) and however it is stored (for example ICT system/database, cloud storage, council drive filing structure, email, filing cabinet, shelving and personal filing drawers.)

This policy does not apply to information held by schools who are separate data controllers and have their own policies.

Related policies and procedures

This policy is part of the Information Governance Framework. Related documents are:

- Special Category Data and Appropriate Policy Document
- Data Breach Procedure
- Data Protection Impact Assessment Procedure
- Subject Access Request Procedure

Responsibilities

Everyone collecting, using, storing and disposing of personal data is responsible for following good data protection practice. All information users with access to council information are responsible for:

- **Members**
  - Complying with this policy when acting as a Member of the Council.
    Note: when acting as a representative of residents of their ward Members are individually responsible for the processing of personal data.
- **Employees** (including temporary employees, contractors, consultants and volunteers)
  - Understanding, and adhering to this policy, the council's ICT acceptable use policy and any other relevant council policies, procedures and guidance relating to data protection and information handling
  - Completing data protection training
- **Managers**
  - Implementing data protection policies and procedures within their areas and ensuring appropriate resources are available for this

Some roles have specific responsibilities:

- **Corporate Management Team** - by demonstrating the Council's commitment to accountability and promoting good governance, CMT have the lead role in developing a data protection culture within the Council.
- **Senior Information Risk Owner (SIRO)** – the SIRO has overall responsibility for the Council's compliance with data protection legislation and this policy. **The SIRO for Gateshead Council is the Strategic Director of Corporate Services and Governance**.
- **Caldicott Guardian** – a senior person responsible for protecting the confidentiality of patient and service-user information for Health and Social Care and enabling appropriate information sharing. The Guardian plays a key role in ensuring that the Council and partner organisations satisfy the highest practical standards for handling patient identifiable information. Their remit covers all social care records for children and adults. **The Caldicott Guardian in Gateshead Council is the Strategic Director of Integrated Adults and Social Care Services**.
- **Data Protection Officer -** The council employs a suitably qualified/experienced Data Protection Officer (DPO). The DPO advises the council on all matters relating to data protection and compliance with the relevant laws. **The DPO sits within Legal & Democratic Services**. The DPO leads the DPO team which provides operational and

strategic advice and support to services in respect of data protection and wider information governance matters. The DPO's role is defined by the GDPR and is to:

- inform and advise about the obligations to comply with the UK GDPR and other data protection laws;
- monitor compliance with the UK GDPR and other data protection laws, and with the Council's data protection policies, including managing internal data protection activities; raising awareness of data protection issues, training staff and conducting internal audits;
- to advise on, and to monitor data protection impact assessments;
- to cooperate with the ICO; and
- to be the first point of contact for the ICO and for individuals whose data is processed (employees, customers etc).

The DPO / DPO team can be contacted by email at DPOcouncil@gateshead.gov.uk

- **Information Asset Owners** (**IAOs - Service Directors**) are responsible for ensuring that the council's data protection policies, procedures and approach of data protection by design are communicated and implemented within their area of responsibility. IAOs are also responsible for records management and document retention guidelines within their service.

Data protection objectives

The Council's data protection objectives are to:

- Protect the confidentiality and integrity of personal data
- Build and maintain the confidence of service users in the Council as a trusted partner through the correct and lawful treatment of personal data
- Fulfil its responsibilities as a data controller under the GDPR

The Council will meet these objectives through applying the data protection principles, complying with other requirements of data protection legislation, and having due regard to guidance from the Information Commissioner's Office (ICO) on best practice.

Data protection principles

All processing of personal data will follow the data protection principles set out in the GDPR.

Lawfulness, fairness and transparency

Personal data processing must be lawful and transparent, ensuring fairness towards the individuals whose personal data is being processed. Personal data should only be collected, stored and processed when the legal basis relied on under GDPR has been identified and documented. Data subjects must be provided with specific detailed information about the processing in the form of a privacy notice.

Purpose limitation

Specific purposes must be identified for processing personal data and individuals must be told of these when collecting their data. Personal data cannot be used for other purposes that are incompatible with this original purpose.

Data minimisation
Only the personal data necessary to fulfil the identified purpose must be collected. Data must be adequate, relevant and limited to what is necessary. When no longer required for the specified purpose data should be deleted or anonymized in accordance with retention guidelines.

Accuracy
Personal data must be accurate, kept up-to-date, and corrected if it is found to be inaccurate for its intended purpose.

Storage limitation
Personal data must not be stored for longer than necessary for the purposes for which it was collected including for the purpose of legal, accounting or reporting requirements.

Security, integrity and confidentiality
Personal data must be secured by appropriate technical and organizational measures against unauthorized or unlawful processing, and against accidental loss, destruction or damage. These security measures will protect the confidentiality, integrity and availability of personal data processed by the Council.

Accountability
Data controllers must take responsibility for their use of personal data and compliance with the other principles. They must have appropriate measures and records in place to be able to demonstrate that compliance. The Council will demonstrate compliance by maintaining documentation including policies, procedures, privacy notices, records of processing activity, logs of incidents and information requests, and, sharing agreements.

Special category data and criminal offence data

Some personal data is more sensitive. The GDPR sets additional conditions for the processing of special category data and criminal offence data.

The Council recognises the more sensitive nature of special category data and criminal offence data. All data is stored securely and only necessary special category data is collected by the council, its staff, councillors and partners/contractors.

The council will only process special category data and criminal offence data if the conditions of the GDPR are met or an exemption listed in the DPA applies. The Council is obliged by law to document how we process special category data and criminal offence data (refer to the Special Category Data and Appropriate Policy document for details).

Consent

One of the lawful bases for processing personal data set out in the GDPR is consent. To be valid under GDPR, consent from the data subject for processing must be:

- Obtained by opt-in through an affirmative action
- Fully informed
- Not subject to conditions
- Specific – kept separate from any other matters
- Easily withdrawn at any time at which point further processing must cease.

If you intend to process the personal data for a different and incompatible purpose which was not disclosed when the Data Subject first consented you will need to seek fresh consent.

Consent for the processing of special category data must be explicit, that is set out in a clear and explicit statement with an affirmative action from the data subject.

The Council will keep records of all consents obtained to demonstrate compliance with consent requirements.

Privacy Notices

The law requires certain information to be given to individuals at the point their personal data is collected. The Council will publish all privacy notices on its website. There is a corporate privacy notice together with specific privacy notices for each service which collects and processes personal data. The notices provide transparency to individuals as to what data is collected, by whom, from what purpose, which third parties it may be shared with, how long the information will be held and what data subject rights are available.

Privacy by design and data protection impact assessments

The Council will keep data protection at the heart of service design and delivery which includes undertaking data protection impact assessments (DPIA) for any new work which meets the basic assessment criteria (refer to the Council's DPIA Procedure). This approach ensures staff consider, up front, how our processing will impact on the individuals whose data we use and take steps to ensure data is as secure as possible throughout.

Record of Processing Activities (RoPA)

The GDPR requires the Council to record all processing activities. Each team within the Council has a RoPA which records what personal data is held, where it is held, what is done with that data, who it is shared with (including any international transfers), the lawful basis for processing the data and retention periods. This record has been prepared using an Information Asset Register which records all information held by each team (not just personal data).

Data Subject Rights

The Council will ensure procedures are in place so that individuals can exercise their rights regarding their personal data, including the rights of access, rectification, erasure, restriction, data portability, objection and those related to automated decision-making.

Information sharing with other organisations

The Council shares data with other organisations for multiple purposes but will do so only when a lawful basis for this sharing exists. The Council will be transparent and as open as possible about how and with whom data is shared; with what authority; and for what purpose; and with what protections and safeguards. When information is regularly shared with other organisations or partners such as other Local Authorities, the Police, the NHS and voluntary organisations, specific protocols will be agreed and an information sharing agreement put in place and signed by all parties. Responsibility for implementation of the agreement will lie with the Information Asset Owner. Guidance on disclosing personal data in response to one-off information requests from other organisations (those not covered by protocols) will be provided on the Intranet.

Controller-processor arrangements

When external providers process data on behalf of the council, including the use of cloud-based services, ownership of the personal data remains with the Council as data controller. In such cases, the Council determines the purposes and the manner of the processing. Formal data processing agreements will be put in place with organisations that process personal data on the Council's behalf (Data Processors) before any processing commences. The data processing agreement will contain the terms specified by the GDPR and detail the extent of the processing activity. Where necessary, additional safeguards will be put in place for more sensitive data processing.

When the Council acts as a data processor (for example in providing services to schools) it will enter a data processing agreement with the data controller.

Notification of personal data breaches

Personal data breaches will be recorded and will be reported to the Information Commissioner's Office (ICO) and affected individuals (if the relevant threshold for risk or harm is reached). (Refer to the council Data Breach Procedure)

Complying with the GDPR's restrictions on transfers of personal data outside of the UK.

The Council will have due regard to and comply with requirements of the GDPR for the security of transfers of personal data outside of the UK.

Automated processing and automatic decision making

A DPIA must be carried out before any automated processing (including profiling) or ADM activities are undertaken. The Council will fully inform data subjects of any automated processing and ensure suitable measures are put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

Information Commissioners Office (ICO)

The Council is registered with the Information Commissioners Office (ICO) who is the Supervisory Authority. The councillors of Gateshead Council, although data controllers in their own right, are exempt from registration. The Electoral Registration Officer (ERO) for Gateshead is independently registered with the ICO as are any wholly owned companies of the Council.

Training and awareness

All staff will undertake annual mandatory data protection training including advice on how and when they should contact the council's DPO.

Audit and review of data protection

The Council's internal audit function will carry out regular systematic audit of processes to ensure the council's teams maintain compliance with data protection legislation and are operating within best practice wherever possible.

Data protection is part of information governance and governed by structures described in the Information Governance Framework.

Data protection policies and associated procedures are adopted by the Council and will be regularly reviewed by the DPO. Complaints about responses to subject access requests and how the council processes data under the GDPR will be investigated by the DPO.

Breach of policy

Failure to adhere to the standards set out in this policy may result in the Council breaching its obligations under the GDPR and the possibility of regulatory action from the ICO. Breaches of this policy must be reported to the DPO and may be subject to disciplinary proceedings.

This policy is designed to ensure effective data protection practice, failure to adhere to the practices in this policy increases the likelihood of a personal data breach occurring. All personal data breaches must be reported to the DPO using the council's Personal Data Breach Procedure and will be investigated accordingly. The council will always treat any data breach as a serious issue, potentially warranting a disciplinary investigation. Each incident will be investigated, judged on its individual circumstances and addressed accordingly.

Review of policy

This policy will be reviewed as it is deemed appropriate, but no less frequently than every 2 years.

Appendix 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 UK 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.

Criminal Offence Data: personal data relating to criminal convictions and offences, including personal data relating to criminal allegations, investigations and proceedings.

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. The Council is the Controller of all Personal Data relating to our employees and Personal Data used in our business for our own purposes.

Data processor: Processors act on behalf of the relevant controller and under their authority. In doing so, they serve the controller's interests rather than their own. A processor should only process personal data in line with a controller's instructions unless it is required to do otherwise by law.

Data Privacy Impact Assessment (DPIA): assessment used to identify and reduce risks of a data processing activity. A DPIA is mandatory for processing that is likely to result in a high risk to individuals and should also be conducted whenever a process, system, project or work activity that could have an impact on the privacy of individuals or risks to their personal data is implemented or changed.

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.

Personal data: Personal data means data which relate to a living individual who can be identified: a) from those data, or b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller, and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.

Privacy Notices: separate notices setting out information that should be provided to Data Subjects when the Company 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
- 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.

Special category 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.