Guildford Borough Council

Privacy and Data Protection Policy

Origination/author:	Ciaran Ward, Information Governance/Data Protection Officer
Policy Owner – Service:	Strategy and Communications
This document replaces:	Privacy and Data Protection Policy 2018-2021
Committee approval:	Tbc
Last Review Date:	2021
Next Review Date:	2025

Contents

1) Introduction

Guildford Borough Council is committed to fulfilling its obligations under Data Protection law, namely the General Data Protection Regulation (GDPR) and has produced this policy to provide assurance to customers and residents and, along with associated practice notes to assist officers and councillors.

The Council's mission within its Corporate Plan 2021-2025 is to be "an efficient, innovative and transparent Council that listens and responds quickly to the needs of our community." This policy will contribute to the council's strategic priorities by ensuring we handle personal information securely and efficiently.

This document is one of a group of policies falling under the Council's Information Security Framework and is subject to ongoing review in the light of changes in the law and Information Commissioner's guidance.

This policy applies to all employees, councillors, volunteers, and contractors of Guildford Borough Council.

Key definitions:

- A **controller** determines the purposes and means of processing personal data.
- A **processor** is responsible for processing personal data on behalf of a controller
- A **data subject** means an individual who is the subject of personal information
- **Personal data** means any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier.
- A **personal data breach** means 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.

Corporate Technical and Legal Guidance which forms part of this policy includes (but is not limited to):

1. CCTV
2. Council Tax information
3. Councillors and Elected Officials
4. Electoral Register information
5. Information sharing and information sharing protocols
6. International Transfers
7. Marketing
8. Personal contact lists
9. Personal information online and use of cookies
10. Photographs and Photographers
11. Privacy Impact Assessments (PIAs)
12. Publicising legal action against individuals
13. Sensitive personal information
14. Use of appropriate privacy notices.

A quick reference guidance for staff is included at Appendix 1 of this policy.

2) Our commitment to Data Protection

In order to provide services, Guildford Borough Council needs to collect and use certain types of information. This includes information relating to members of the public, clients and customers, current, past and prospective employees, suppliers (such as sole traders) and other individuals.

The Council must also collect and use certain types of information to comply with the law – examples would include Council Tax and Electoral Register information.

Guildford Borough Council will use personal information properly and securely regardless of the method by which it is collected, recorded and used and whether it is held on paper, on a computer or network or recorded on other material such as audio or visual media such as CCTV.

Guildford Borough Council regards the lawful and good management of personal information as crucial to the successful and efficient performance of the Council's functions, and to maintaining confidence between residents, customers and ourselves. We ensure that our Council treats personal information lawfully and correctly and respects privacy.

To this end, Guildford Borough Council fully endorses and adheres to the principles of Data Protection, as set out in Article 5 of the GDPR.

In addition, Guildford Borough Council will ensure that:

- there is someone who monitors internal compliance, informs and advises the Council on its data protection obligations and acts as a contact point for the public and the supervisory authority (Information Commissioner's Office, ICO). This person is the Data Protection Officer (DPO);

- everyone managing and handling personal information understands that they are contractually responsible for following good data protection practice;

- everyone managing and handling personal information is appropriately trained to do so;

- everyone managing and handling personal information is appropriately supervised;

- anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;

- queries about the handling of personal information are promptly and courteously dealt with;

- methods of handling personal information are regularly assessed and evaluated.

3) The GDPR Data Protection Principles

The following legally binding good-practice principles govern the way the Council manages personal information.

Personal information:-

1. processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');

2. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes ('purpose limitation');

3. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation');

4. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay ('accuracy');

5. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes 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 historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation 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');

6. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

4) The Standards Adopted

Guildford Borough Council will, through appropriate local management and application of corporate criteria and controls:

- fully observe regulations and codes of practice regarding the fair collection and use of personal information (this includes but is not limited to codes of practice issued by the Information Commissioner);

- specify the purposes for which personal information is or will be used through registration with the Information Commissioner and through appropriate use of privacy notices on application forms, web pages and via telephone, in other words, through whatever means personal information is collected;

- only collect and process appropriate information to the extent needed to fulfil operational or service needs or to comply with any legal requirements;

- check and maintain the quality of information used;
- apply checks to determine the length of time information is held regardless of its format. This will be addressed by a corporate Data Retention Policy and local procedures to establish and keep to appropriate retention periods;
- ensure that the rights of people about whom information is held can be fully exercised under the Act;
- take appropriate technical and organisational security measures to safeguard personal information specifically by means of an Information Security Framework supported by each service's local procedures;
- ensure that personal information is not transferred abroad without suitable safeguards.

5) Overview of Roles and Responsibilities

All Staff will:

(a) ensure they understand how this policy, its associated guidance notes and their local working procedures affect their work.

(b) assess the kind of information they use whilst carrying out their work and whether they have responsibility for any personal information.

(c) make sure that they use personal information in accordance with this policy, its associated guidance notes and their local working procedures.

Heads of Service will:

(a) identify the services they provide and any specific processes they are responsible for that involve the use of personal information.

(b) appoint at least one Privacy and Information Security Champion for their Service.

(c) appoint one or, where appropriate, more information asset owners (sometimes referred to as "Responsible Officers") who will be responsible for each information asset or system within the service.

(d) make the Information Governance Officer (via their Privacy and Security Champion(s)) aware of all of their systems that use personal information, This is so that the Information Governance Officer may notify the Information Commissioner, as required by law.

(e) carry out a Data Privacy Impact Assessment (DPIA) in relation to each new project or proposal that will involve the use of personal information or affect privacy. This must be carried out at the beginning and at any review of the project, not "bolted on" at the end. The Information Governance Officer must be informed at an early stage.

(f) document local working procedures to ensure staff (including temporary staff) who have access to personal information systems are aware of the steps they must take to

comply with the data protection legislation. (Bear in mind staff vetting requirements required by the Information Security Framework).

(g) train or arrange training for staff in relation to local working procedures.

HR Services will ensure the following arrangements are in place:

(a) baseline personnel checks at recruitment, to ensure that new members of staff are made aware of this policy document at induction stage and also that a specific condition is included in contracts of employment;

(b) (the Data Protection team must be informed of new starters and leavers, temporary/contract staff who require training are provided with the relevant policies and procedures before being given access to personal data; and
(c) For managers to ensure all new starters with an email account undertake and pass the GDPR E-Learning module within their first month of employment.

Data Protection Team

This team comprises:

- Senior Information Risk Owner (SIRO)
- Data Protection Officer (DPO)
- Information Assurance Manager (IAM)
- Information Governance Officer (IGO)

The Senior Information Risk Owner will:

(a) establish an information risk strategy which allows assets to be exploited and manages risks effectively

(b) identify business-critical information assets and set objectives, priorities and plans to maximise the use of information as a business asset

(c) establish and maintain an appropriate risk appetite with proportionate risk boundaries and tolerances.

(d) establish an effective Information Governance Framework

(e) act as the champion for information risk within the Council, being an exemplar for all staff and encouraging CMT to do likewise

(f) build networks with peers and organisations that can provide essential support and knowledge exchange services

(g) ensure compliance with regulatory, statutory and organisational information security policies and standards

(h) ensure all staff are aware of the necessity for information assurance and the risks affecting the Council's corporate information

(i) establish a reporting and learning culture to allow the Council to understand where problems exist and develop strategies (policies, procedures and awareness campaigns) to prevent data related incidents in the future.

The Data Protection Officer

(a) is independent
(b) reports to Senior Management
(c) monitors the Council's compliance with the GDPR;
(d) is the Council's representative to the Information Commissioner's Office.

You can report a personal data breach to the DPO at DPO@guildford.gov.uk.

The Information Assurance Manager will:

(a) support the Service Assurance function in implementing the Information and Communications Technology (ICT) security vision, model and principles across all of Guildford Borough Council, ensuring compliance with Payment Card Industry Data Security Standard, General Data Protection Regulation and other appropriate industry standards, to support the organisational strategy.

(b) work with the ICT department to guide the selection and deployment of appropriate technical controls to meet specific security requirements and define processes and standards to ensure that security configurations are maintained. The Information Assurance Manager is also responsible for managing Guildford Borough Council's information security systems through the implementation of ISO27001.

The Information Governance Officer will

(a) ensure that the Data Protection Policy and associated documents are kept up to date and communicated to staff in an appropriate manner.

(b) provide technical and legal guidance on specific sectors and issues and will keep such guidance up to date.

(c) arrange for the provision of advice and training to staff on request.

(d) be responsible for notification of the Council's processing to the Information Commissioner.

Privacy and Information Security Champions will:

(a) co-ordinate Data Protection matters for the Service they represent.

(b) ensure that decisions, guidance and policy matters are communicated to service management teams and the relevant staff in the service they represent.

(c) inform the Information Governance Officer of specific matters within the Service that require specialist advice or guidance.

The above objectives are facilitated by the Privacy Information Group, which is chaired monthly by the Information Governance Officer and consists of representatives from each service area.

Information Risk Group (IRG)

The IRG is chaired monthly by the Council's SIRO and includes the ICT Manger, DPO, IAM and IGO. The IRG's role is to identify risk and provide advice on the effective management of all Council-held information by ensuring compliance with relevant legislation and effective risk management.

6) PCI DSS Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements designed to ensure that all organisations who process, store or transmit credit or debit card information maintain a data secure environment. Payment cards and payment transactions will contain sensitive personal data. Sensitive card/payment data can include but is not limited to the name on the face of the card, the Primary Account Number (PAN), Card Validation Code (CVC, CVV2, CVC2), and any form of magnetic stripe data from the card (Track 1, Track 2).

Payment card and/or payment transaction data stored, processed or transmitted by officers of Guildford Borough Council and/or its authorised contractors/service providers must be protected and security controls must conform to the Payment Card Industry Data Security Standard (PCI DSS). All persons/organisations involved in storing, processing or transmitting personal information through payment cards must comply with the Council's Privacy and Data Protection Policy to ensure the security of the personal information associated with payment cards and/or payment card transactions.

Any officer of Guildford Borough Council commissioning goods and/or services on behalf of the Council must notify the Procurement Team if the procurement will result in payment transactions in addition to the payment for the goods/services. The Procurement Team and/or the Data Protection Team may require any contractor/service provider to undertake a Data Privacy Impact Assessment in order to ensure that such transactions are PCI DSS compliant.

7) Links with Other Policies

This Privacy and Data Protection Policy, as well as the more detailed working procedure documents issued locally, will have an impact on the following policy areas:

- Information Security Framework
- ICT Security Policy
- Acceptable Use of Council ICT Equipment
- Covert Surveillance and use of informants
- Disciplinary Procedures
- Equality and Diversity
- Fraud and Corruption
- Freedom of Information
- Grievance Procedures
- Health & Safety
- ICT Security Policy
- Training and Development
- Violence at Work
- Whistle Blowing.

These policies can be found on the Council's intranet here.

8) Measurement and Impact

We will measure the success of this policy through the annual Data Protection and Information Security Update Report presented to the Corporate Governance and Standards Committee.

Appendix 1: Reference Guide for Guildford Borough Council employees, councillors and contractors

Breaches of the Data Protection Act
All breaches (suspected breach of confidentiality) should be reported to the Data Protection Team as soon as they occur. Please refer to the breach notification procedure for full details.

The Information Governance Officer reports breaches to the Corporate Governance Group on a quarterly basis.

CCTV
Follow the corporate procedure note on authorising CCTV.

Collecting/obtaining personal information
Individuals have a right to know (1) that the Council is using their information, (2) a description of the personal information the Council is using, (3) the purposes for which the information is being used and (4) the recipients (or classes of recipients) to whom the personal information may be disclosed. Whichever means is used by a Council service to collect personal information, the service must provide a privacy notice to the affected individual(s) and this must meet the standards set out in the Information Commissioner's guidance.

Councillors
In terms of Data Protection, Councillors have three distinct roles:

(1) as a member of a Council committee. In this role, they act for the Council and have the same access rights as a member of staff, subject to the "need to know principle".

(2) Political: they act for their political party or, where independent, their own political agenda, and not for the Council. In this role, the Councillor's access rights are the same as for a political party.

(3) as a representative of one or more constituents: In this role they are acting for the member of the public and not for the Council (in a comparable way to, say, the Citizen's Advice Bureau). The Councillor has the same access rights as the constituents he or she is acting for but must demonstrate that the constituent(s) has given consent for them to act for them.

Couriers
Take care when sending protected information via courier. Encrypted email may be safer. If you cannot avoid using a courier, please follow the procedural guidance on the use of photographers.

Information Security
All staff are responsible for ensuring that personal data, which they use, or process is kept securely and is not disclosed to any unauthorised person or organisation. Access to personal data should only be given to those who have and can show a business need for access to the data for the purpose of their duties and the principle of least privilege should be applied.

Please refer to the Council's IT Policies and Procedures which includes the Acceptable Use (of ICT systems and equipment) Policy for the Council's detailed requirements and arrangements.

Information Sharing
Staff will generally share personal data of a customer where the Council is performing tasks that are necessary and carried out in the public interest and also in the exercise of various public functions. For example, the Council's Benefits service will share personal data with the DWP or other public bodies and third parties.

There will also be occasions when it will be necessary for staff to share personal data of a customer to comply with a legal obligation. For example, it may be necessary to share the information to assist the police with a criminal investigation.

If you are ever in doubt about a request to share information please contact the Data Protection team for advice at DPO@guildford.gov.uk.

The Council must only share personal data if it has a lawful basis to do so, where it is necessary to achieve a clear purpose and, with that purpose in mind, it is fair and proportionate to do so. Personal information shared with any Surrey agency must comply with the Surrey Multi Agency Information Sharing Protocol ("Surrey MAISP").

If information is regularly shared with third parties who are not one of the Surrey agencies, Data Sharing Agreements should be in place. However, they are not needed when information is shared in one-off circumstances, but a record of the decision and the reasons for sharing information should be kept. The Data Protection Officer, who will keep a register of all Data Sharing Agreements, must sign off all Data Sharing Agreements.

International Transfers
Before entering into any agreement whereby personal information will be processed on behalf of the Council by another agency, check whether the agency is confined to the European Economic Area. Disclosures to international companies could amount to an international transfer of personal information and this must be accounted for in the written agreement.

Notification
The Council must register with the Information Commissioner its use of personal information and the purposes it uses the information for (this is called "Notification"). Services must therefore inform the Information Governance Officer of any new purposes for which they use personal information (for example if they begin to provide a new service for customers).

Photographs and Photographers
Photographs of people are personal information and can be used in ways detrimental to the subject's privacy. The Council has special procedural rules on the use of photographs and photographers and anyone using this kind of information must comply with them.

Press releases about court cases and other action against individuals
Information about the commission or alleged commission of any offence and any proceedings relating to the alleged or actual offence are subject to special safeguards. Officers must complete a special privacy impact assessment form (see below) for publicising legal action against individuals before they issue any press release. The Information Governance Officer will keep a central record.

Data Privacy Impact Assessments
Project Managers must conduct a Data Privacy Impact Assessment (PIA) before undertaking any new project or new way of working, which will have a bearing on how personal information is used. This is obligatory under Article 35 of the GDPR and will help to ensure that any benefits brought about by the change, is proportionate to the impact on privacy.

Such instances may include, but are not limited to:

1.1.1 Introduction of new technologies;
1.1.2 Systematic and extensive processing activities;
1.1.3 Large scale processing of special categories of data or personal data relating to criminal convictions or offences;
1.1.4 Large scale, systematic monitoring of public areas, such as CCTV; and
1.1.5 Before entering a data sharing agreement.

Retention of records
The Council has a Records Retention and Disposal Policy which should be referred to when considering how long to keep records for.

Staff (information about)
HR and anyone handling personal information about staff must comply with the Information Commissioner's Employment Practices Code.

The rights of data subjects
Subject to the provisions of the legislation, councillors, staff and members of the public have the following 'information rights' in relation to their personal data:

- to be informed about how and why their personal data is processed;
- to access their data;
- to rectification of their data;
- to erasure of their data;
- to restrict processing of their data;
- to data portability;
- to object to processing of their data; and
- not to be subject to fully-automated decision-making including profiling.

The Data Protection Officer will ensure appropriate processes are in place to ensure the Council enables the exercise of these rights, according to the provisions of the legislation.

Any information rights requests are processed by the Information Governance Officer. Individuals will be expected to submit requests in writing and provide any necessary proof of identification as part of the request.

The Council aims to respond promptly to these information rights requests and, in any event, within the statutory time limit (normally 30 days). Requests will be managed and tracked by the Information Governance Officer.

This policy will take effect from (date to be confirmed following approval)