SURREY HEATH BOROUGH COUNCIL

DATA PROTECTION POLICY

Contents

February 2026

Surrey Heath Borough Council
Knoll Road, Camberley GU15 3HD
Information.governance@surreyheath.gov.uk

1. Scope of this policy statement

Surrey Heath Borough Council (SHBC) is committed to fulfilling its obligations under the UK General Data Protection Regulation (UK GDPR), Data Protection Act 2018 (DPA 2018) and the Data Use and Access Act 2025 (DUAA) and has produced this policy to provide assurance to customers and staff and to assist officers. UK GDPR and DPA 2018 need to be considered side by side.

UK GDPR,DPA 2018 and the DUAA, otherwise known as Data Protection legislation, establishes a framework of rights and duties which are designed to safeguard personal data to which SHBC is committed. This framework balances the legitimate needs of the Council to collect and use personal data about the people the Council deals with for business and other purposes against the right of individuals to respect the privacy of their personal details. This includes members of the public, clients and customers, members, current, past and prospective employees, suppliers (such as sole traders) and other individuals with whom the Council communicates.

Surrey Heath Borough Council will use personal information lawfully and securely regardless of the method, by which it is collected, recorded and used and whether it is held on paper, electronically or recorded on other material such as audio, visual media (CCTV) or Body Worn Cameras. This includes use of printers where information is immediately printed to ensure this is conducted in a secure location and never left on printers. The Council will respect the privacy of individuals.

To this end, Surrey Heath Borough Council fully endorses and adheres to the principles of Data Protection, as set out in Article 5 of the UK GDPR (see Section 4).

If any Surrey Heath Borough Council work is outsourced that we ensure the company used complies with the same standards as would be expected if completed by SHBC.

2. Definitions

2.1 Personal Data

'Personal data' under the Data Protection legislation is information about a living individual who can be identified directly or indirectly from the information. The information can be factual information (e.g. names and addresses) or expressions of opinion or intentions about an individual. Other examples of personal data include location data, on-line identifiers (IP addresses and mobile devices ID's and photographs), or identification number such as National Insurance Number.

2.2 Consent

Consent is the fact that permission has been given by a subject matter. A person who consents to something is in effect giving permission for that thing to happen. Explicit consent requires an affirmative action to be taken, this can be articulated either orally or in writing but a clear and voluntary preference is given and it must be given freely where the available option and the consequences have been made clear.

2.3 Data Subject

Data subject means 'an individual who is the subject of personal data'. This must be a living individual.

2.4 Data Controllers and Data Processors

Data Controller is Defined as a person (or organisation) who (either jointly or in common with other persons/organisations) determines the purposes for which, or the manner in which, any personal data are, or are to be, processed. The Data Controller is ultimately responsible for all records processed.

Joint Data Controller determines the purposes and means of processing personal data jointly with another data controller.

Data Processor means any person (other than an employee of the data controller) who processes the data on behalf of the data controller

GDPR puts obligations on both data controllers and data processors to maintain records of personal data and processing activities and they may each be held responsible for a data breach. There are also obligations on data controllers to ensure contracts with processors comply with GDPR principles.

2.5 Data Protection Impact Assessment (DPIA)

A Data Protection Impact Assessment is a process to help the Council identify and minimise the data protection risk of a project. A DPIA must be completed for any new, or change to existing, processing of personal information whereby there may be a risk to the individual.

2.6 Information Asset Register

An information asset is a collection of information, defined and recorded as a single unit so it can be understood, shared, protected and used efficiently to help the Council provide a service. Information assets have recognisable and manageable value, risk, content and lifecycles. Maintaining an Information Asset Register (IAR) is a requirement of the UK GDPR. The IAR is a simple way to help Council Officers understand and manage the Council's information assets and the risks relating to those assets.

Examples of information assets within Surrey Heath are; Uniform, Civica, Complaints CRM, planning application history.

The Council's IAR includes the following information:

- Identification of each information asset
- Where the information is held
- Who the Information Asset Owner is

- Why we keep it
- Who is allowed to access it
- Who we share it with
- How long we keep it

2.7 Processing

Processing is defined as any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.8 Special Category Data

This is personal data consisting of information relating to any of the following:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetics
- Biometrics (where used for ID purposes)
- Health and Social Care
- Sex life
- Sexual orientation

Special category personal data is subject to much stricter conditions of processing. Personal data relating to criminal convictions and offences are not included within special category data per se but similar extra safeguards apply to its processing.

The Council must be able to demonstrate that the processing is strictly necessary and satisfies one of the conditions in Schedule 9 of the UK GDPR or is based on consent.

3. Roles and Responsibilities

3.1 All staff will ensure that:

- they consider whether the information they are working on contains personal data and then use it in accordance with this policy and the six data protection principles of the UK GDPR.
- they complete regular mandatory Data Protection and Information Security training as required
- they follow the Data Protection Policy and understand how it works, disciplinary action may be taken against any council employee who breaches any instruction contained within it, or following from, the UK General Data Protection Regulation and Data Protection Act 2018. Compliance with the Data Protection Policy forms part of Staff Terms and Conditions.

3.2 Data Protection Officer

- this is a statutory post. The Council's Data Protection Officer is the Information Governance Manager
- will inform and advise the Council and its employees about their obligations to comply with both the UK General Data Protection Regulation and the Data Protection Act 2018
- monitor compliance with the Data Protection legislation, including the assignment of responsibilities and audits
- provide advice about Privacy By Design and Data Protection Impact Assessments and monitor their performance
- co-operate with the Information Commissioner's Office (ICO)
- act, where necessary, as the contact point for the ICO on issues relating to the processing of personal data

3.3 Senior Information Risk Owner (SIRO)

- The Councils SIRO is the Director of Finance (Section 151)
- the SIRO has overall strategic responsibility for governance in relation to data protection risks.
- act as advocate for information risk in the Corporate Management Team
- include information risk in the Annual Governance statement
- review information management on the Corporate Risk Register
- in liaison with the Data Protection Officer, Information Governance Manager and Heads of Service ensure the Information Asset Owner roles are in place to support the SIRO role

3.4 Information Asset Owners (IAO)

- these are members of the Wider Management Team. Their role have oversight of data protection compliance and to understand what information is held by their service, what is added and removed, how information is moved and who has access and why. They will assist in the production of the Information Asset Register and agree and sign off their service's register which include the retention and disposal schedule for their service

3.5 Directors/Heads of Service will:

- ensure compliance with Data Protection legislation within their services and liaise with the Data Protection Officer where necessary
- identify the services they provide and any specific processes they are responsible for that involves the use of personal information
- appoint, when required, any Information Asset Owners for their services who will be responsible for each information asset or system within the service
- review any new project, where personal data is being collected, and consider and build in privacy from the beginning. This is called Privacy By Design and is a requirement of UK GDPR.
- consider the requirement for a Data Protection Impact Assessment where any processing of personal information will be undertaken on a regular basis e.g. involving IT systems, third part sharing, CCTV or body

worn cameras whereby there may be a risk to the individual. The Information Governance Manager must be informed and involved at an early stage.
- ensure staff complete any mandatory data protection training
- ensure contracts, where personal data processing is involved, adequately covers data protection, including if a data processor is involved, they are made aware of their responsibilities under data protection legislation.

3.6 HR service will ensure the following arrangements are in place:

- where necessary, ensure baseline security checks (personnel checks for prospective staff) are carried during the recruitment process
- to ensure that new members of staff are made aware of this policy document at induction stage
- to ensure that all new starters and temporary staff complete Data Protection and Information Security e-learning training as part of their induction.

3.7 ICT Manager

- Responsible for creating, implementing and maintaining the Council's Information Security Policy to reflect changing local and national information security requirements.
- Reviewing with the Information Governance Manager the requirement for a DPIA when new systems are installed.

3.8 The Information Governance Manager will:

- Act as Data Protection Officer and carry out day to day duties, including liaising with the ICO
- ensure that the Data Protection Policy and associated documents are kept up to date and communicated to staff in an appropriate manner
- provide technical guidance on specific sectors and issues and will keep such guidance up to date
- arrange and carry out the provision of advice and training to staff

- be responsible for notifying that the Council holds personal information about living people and the payment of the registration fee to the Information Commissioner's Office in accordance with the Data Protection (Charges and Information) Regulation 2018 and keeping an internal record in relation to all personal data processed
- manage and complete subject access requests. Enquiries about Data Protection should be addressed to the data protection mailbox
- keep up to date with changes in the law and guidance on Data Protection legislation
- advise on and ensure any data sharing is compliant with the UK General Data Protection Regulation and Data Protection Act 2018 including Schedule 2, Part 1, Paragraph 2 requests
- advise on and draft, as required, Data Sharing Agreements and DPIA's

4. Data Protection Principles (Article 5 of the General Data Protection Regulation)

UK GDPR applies to any processing of personal information and requires compliance with the Data Protection principles as set out in Article 5 of the GDPR. The six principles lie at the heart of the UK GDPR. Processing includes virtually anything that can be applied to information, including acquisition, storage and destruction as well as active use. This includes electronic systems, hardcopy records, CCTV images, photographs and digital images.

The data protection principles require that personal data should be:

a) processed lawfully, fairly and in a transparent manner
b) collected for specified, explicit and legitimate purposes only also known as 'purpose limitation'
c) adequate, relevant and limited to what is necessary
d) accurate and where necessary kept up to date
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data are processed and

f) 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').

Anyone who processes personal data about people must make sure that:

- they respect the individual's data protection rights
- they are transparent about how they use personal data and not process data in a way that is unduly detrimental, unexpected or misleading to the individual concerned
- all electronic and manual filing systems conform to the six Data Protection Principles
- be accountable and able to demonstrate, where necessary, compliance with the principles. Accountability is central to UK GDPR.

5. Lawful basis for processing

The lawful basis for processing (using) personal data is set out in the UK GDPR **Article 6**. At least one of these must apply to allow the Council to process personal information:

a) **Consent**: the data subject has given clear and unambiguous consent for the Council to process his/her personal data for a specific purpose. Another lawful basis should be considered before using this one

b) **Contract**: the processing is necessary for a contract that the Council has with the data subject, or because the data subject has asked the Council to take specific steps before entering into a contract

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

d) **Vital interest**: the processing is necessary to protect someone's life

e) **Public interest**: the processing is necessary for the Council to perform a task in the public interest or in the exercise of official authority vested in the Council

f) **Legitimate interest**: the processing is necessary for the purposes of legitimate interests pursued by the Council or a third party except where such interests are overridden by the interests of the data subject. This requires balancing the Council's interests against the individual's interests. However, this basis is not available to processing carried out in performance of our public task

If processing **Special Category information**, this requires at least one further condition to be satisfied under UK GDPR **Article 9.** Processing of special category data cannot occur unless one of the following applies:

(a) the data subject has given explicit consent. Explicit consent must be expressly confirmed in words. Individuals do not have to write the consent statement in their own words; you can write it for them. However, you need to make sure that the data subjects can clearly indicate that they agree to the statement – for example by signing their name or ticking a box next to it.

(b) processing is necessary for employment, social security and social protection law.

(c) processing is necessary to protect the vital interests of any individual where the data subject is incapable of giving consent. You cannot use this lawful basis in advance of an emergency situation if the data subject can give consent.

(d) processing for the legitimate interests of a foundation, association or any other not for profit body with a political, philosophical religious or trade union aim.

(e) information has already been made public by the data subject

(f) processing is necessary for the establishment, exercise or defence of legal claims or court action

(g) necessary for reasons of substantial public interest, such as:

- i employment, social security and social protection
- ii health and social care purposes
- iii research
- iv statutory government purposes
- v equality of opportunity or treatment
- vi racial and ethnic diversity at senior levels of organisations
- vii preventing or detecting unlawful acts
- viii protecting the public against dishonesty and preventing fraud
- ix support for individuals with a disability or medical condition
- x safeguarding of children and of individuals at risk
- xi information provided to elected representative

(h) preventative or occupation medicine

(i) public health

(j) archiving and research

6. Surrey Heath Borough Council's commitment to Data Protection

Surrey Heath Borough Council is a Data Controller as defined in the UK GDPR and DPA 2018 and is registered with the Information Commissioner's Office and as such all officers, contractors and volunteers have a responsibility for data protection.

Surrey Heath Borough Council is committed to compliance with Data Protection legislation. The Council will carry out the following:

- Appoint a Data Protection Officer (DPO)
- 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)

- meet its legal obligations to specify the purposes for which information is used through the appropriate use of Privacy Notices on application forms, web pages, CCTV signs and via telephone. In other words through whatever means personal information is collected

- collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements, i.e. not collect information excessively or "just in case"

- check and maintain the quality of information used

- ensure adequate recordkeeping for personal data

- apply checks to determine the length of time information is held, ensuring it is up to date and is not kept for longer than is necessary regardless of its format. Members of staff will adhere to the Council's Retention and Disposal Policy to ensure the information is held for only as long as is necessary.

- ensures every person managing and handling personal information is appropriately trained to do so

- ensure that the rights of people about whom information is held can be fully exercised under the legislation

- take appropriate technical and organisational security measures to safeguard personal information specifically by means of the Information Security Policy, Email Security Policy and subsidiary policies

- not disclose personal data, either within or outside the organisation, to any unauthorised recipient. Breaches will be managed in line with the Data Security Breach Policy and Procedure

- ensure that personal information is not transferred outside of the European Economic Area, including storing information in the Cloud, without suitable safeguards. Discussions will take place with the Data Protection Officer and Information Governance Manager before transferring any information overseas

7. Rights of Data Subjects

7.1 The UK GDPR has enhanced individuals rights concerning their personal data. Their rights are as follows:

- the right to be informed about how their information will be used
- the right of access to their personal information (normally known as Subject Access Requests (SAR))
- the right to rectification, which is the right to require the Council to correct any inaccuracies
- the right to request the erasure of any personal information held by the Council where the Council no longer has a basis to hold the information
- the right to request that the processing of their information is restricted
- the right to data portability
- the right to object to the Council processing their personal information
- rights in relation to automated decision making and profiling

7.2 Individuals have the right to be informed about the collection and use of their personal data at the time their information is collected, this is usually via a Privacy Notice. If you have not received the information directly from the data subject then you must provide a Privacy Notice within 1 calendar month or when you first communicate with the data subject or share their data with a third party, whichever is sooner.

The Councils Privacy Notice is located on the Councils website and includes relevant departmental Privacy Notices. You should ensure that

when personal data is collected you provide the data subject with a Privacy Notice either via a link or hardcopy.

7.3 Data subjects (this includes employees and councillors) have the right to access personal data held about them (this includes factual information, expression of opinion, and the intentions of the Council in relation to them, irrespective of when the information was recorded or on what medium), the right to prevent processing likely to cause damage or distress and the right to have inaccurate data rectified, blocked, erased or destroyed.

The Council will arrange for the data subject to see or hear all personal data held about them as long as it does not adversely affect the rights and freedoms of others, and no restrictions apply which prevent disclosure of the personal data. The information will be provided within 1 calendar month of a Subject Access Request being received in writing including, where necessary, two pieces of information to prove identity.

Where the Council is unable to process the request within the timeframe, the data subject will be notified as soon as possible of any potential delay, the reasons for such a delay, and the date when their information will be made available. The Council may extend the time period for processing and responding to a request by a further two months depending upon the complexity. Where a data subject request is considered unfounded or excessive, the data controller may either:

- charge a reasonable fee to provide the information, or
- refuse to act on the request

7.4 Exemptions to the rights

Not all rights are absolute and will depend upon the lawful basis on which the Council is relying to process the personal data.

There are a few circumstances where the rights of the data subject can be overridden such as where the following would occur;

- Providing the information would be likely to prejudice crime or taxation
- Processing is in relation to legal proceedings or court records
- In connection with health and safety

There are further exemptions to the right to be informed and right of access. For example:

- data processed for the purposes of management forecasting or management planning in relation to a business
- personal data that consists of records of the intentions of the controller in relation to any negotiations with the data subject which would be prejudicial to disclose
- personal data consisting of a reference given (or to be given) in confidence

There are further exemptions that only apply to the right of access such as:

- Where a relevant professional has confirmed that disclosing data concerning the data subject's health or social care records is likely to result in serious harm to themselves or others. Please note, where we hold information relating to the data subject's health or social care, which was provided by a relevant professional, it should not be disclosed to the data subject without the approval of that professional, unless we have evidence that the data subject is already aware of the information
- Disclosing information to the data subject would involve disclosing personal data of a third party without their consent and it is not reasonable to do so
- If the third party is a health professional, social worker, or education worker then you do not need their consent to disclose their name in relation to information about the data subject

Decisions will be made on a case by case basis.

7.5 Any queries regarding individual rights under Data Protection, or any requests for personal information whether from the person themselves or from a third party must be referred to the Information Governance Manager or the data.protection@surreyheath.gov.uk email.

8. Data sharing and data matching

8.1 **Unauthorised disclosure** of personal data is a criminal offence. Such data may only be disclosed for registered purposes to:

- the person themselves
- employees of the Council as required in the course of their duties
- members of the Council whereby a UK GDPR Article 6 or Article 9 legal basis applies
- promote the prevention and detection of fraud and crime
- the Courts under direction of a Court Order
- Other Government authorities whereby there is a legal or statutory requirement
- Third parties whereby a UK GDPR Article 6 or Article 9 legal basis applies.

It is important to be aware that just because the information is held by a Council department does not entail that the information can be disclosed internally or freely used for purposes which are not compatible with the reason the information was collected in the first place.

8.2 **Information sharing protocols and/or sharing agreement** must be in place before personal information can be routinely or mass shared with other agencies or third parties, unless required to do so by law. These protocols will be reviewed, amended and updated on a regular basis. They must comply with the Information Commissioner's Data Sharing Code.

8.3 **Surrey Multi Agency Information Sharing Policy (MAISP)** A number of Surrey authorities and agencies including SHBC are signed up to the MAISP, these protocols allow for the safe and legal sharing of personal data and any sharing undertaken under the MAISP must comply with the protocols. A list of the signatories can be found on the Surrey County Council website.

8.4 The Council is required to collect, use and share certain types of personal information to comply with different laws – examples would include Council Tax and Electoral Registration information.

8.5 The Council will comply with the Information Commissioner's guidance on data matching. The Council is a participant of the National Fraud Initiative and the Surrey Counter Fraud Partnership.

9. Contractual and partnership arrangements

In the event that the Council enters into a contract with a third party which involves, collecting, processing, handling, securing or disposing of information at any level there needs to be contractually binding data protection clause in the contract. Specific care should be taken in respect of services provided online and via 'the cloud'.

Such mandatory provisions will identify the roles and responsibilities of the "data controller" and "data processor" in relation to activities carried out during the life, and after termination of, the contract.

Where the parties are data controllers jointly or in common, the Council will liaise with the other relevant parties to ensure that all processing complies with DPA 2018. The responsibilities of each data controller should be expressly and clearly laid out.

Contracts must include as a minimum, the following terms, requiring the processor to:

- only act on the written instructions of the controller.
- ensure that people processing the data are subject to a duty of confidence.
- take appropriate measures to ensure the security of processing.
- only engage sub-processors with the prior consent of the controller and under a written contract.
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR.
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments.
- delete or return all personal data to the controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

10. Training

Data Protection and Information Security training is mandatory for all employees of the Council.

All new employees must complete Data Protection and Information Security e-learning as part of their induction.

All employees must complete the Data Protection and Information Security e-learning package or attend a refresher course annually.

Separate training will be arranged for Members at induction.

11. Links with other policies

The Data Protection Policy will have an impact and relationship with the following policies:

- Information Security Policy
- Data Security Breach Management Policy and Procedure
- Speak up Policy
- Social Media Policy
- Capability Policy
- Recruitment Policy and Procedure
- Regulatory and Investigatory Powers Act 2000 Policy and Procedure
- Homeworking Policy
- Data Protection Policy for Home Working
- Off-site Working Policy
- Disciplinary Policy and Procedure
- Grievance Policy and Procedure
- Anti-fraud and Corruption Policy
- Individual Rights Procedures
- Email Security Policy

12. Review

12.1 A policy review will take place 3 yearly or after legislative changes, important changes in case law or guidance.

Document history

Date	Version	Author	Changes made
15th October 2018	Draft 5.1	Geraldine Sharman	Initial revision of 2017 policy
26 October 2018	Draft 5.2	Geraldine Sharman	Reviewed and written policy
17 January 2019	Version 5	Geraldine Sharman	Approved version
Feb 2021	Version 5	Sally Turnbull	Review
Feb 2022	Version 5	Sally Turnbull	Review
June 2023	Version 5	Sally Turnbull	Review approved by CMT June 2023
February 2026	Version 5	Sally Turnbull	Review