Surrey Heath Borough Council – Privacy Notice

Purpose of this Privacy Notice

This privacy notice aims to give you information on how Surrey Heath Borough Council collects and processes your personal data as part of our public task and through your use of Council services.

It is important that you read this privacy notice and any other notices we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data.

Data Controller

Surrey Heath Borough Council is the data controller and responsible for looking after your personal data (collectively referred to as ”SHBC”, “we”, “us” or “our” in this privacy notice). Occasionally certain services will require us to be Joint Data Controller with others. If this is the case, we will tell you.

We have appointed a Data Protection Officer (DPO) who is responsible for overseeing questions in relation to this privacy notice. If you have any questions about this privacy notice, please contact the DPO using the details set out below.

Contact details for DPO

Full name: Gavin Ramtohal
Name or title of DPO: Head of Legal Services
Email address: **data.protection@surreyheath.gov.uk**
Postal address: Surrey Heath House, Knoll Road, Camberley, Surrey, GU15 3HD
Telephone number: 01276 707100

As part of Surrey Heath’s transparency and accountability, when dealing with people’s data both the Council and the Councillors are registered with the Information Commissioner Office. Each Councillor is registered independently to allow Councillors to consider residents in their local wards personal information when representing them.

You have the right to make a complaint at any time to the Information Commissioner’s Office (ICO), the UK supervisory authority for data protection issues (**www.ico.org.uk**). However, it is usually a requirement of the ICO that we have had the opportunity to satisfy your concerns before you approach them so please contact us in the first instance.

Data we collect about you and how it's collected

Personal data, or personal information, means anything that will identify you.

We may collect, use, store and transfer different kinds of personal data about you; the type of data we are likely to collect includes:

- **Identity Data**; including [first name, maiden name, last name, username or similar identifier, marital status, title, date of birth and gender].
- **Contact Data**; including [billing address, delivery address, email address and telephone numbers].
- **Financial Data**; including [bank account and payment card details].
- **Transaction Data;** including [details about payments to and from you and other details of products and services you have purchased from us].

- **Profile Data;** includes [your username and password, purchases or orders made by you, your interests, preferences, feedback and survey responses].
- **Usage Data**; includes [your preferences in receiving marketing from us and our third parties and your communication preferences].
- **Marketing and Communications Data**; includes [your preferences in receiving marketing form us and our third parties and your communication preferences].

This list does not represent all of the information the Council collects. Please see the Privacy Notices for the individual services for a comprehensive record.

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identity, Contact and Financial Data by filling in forms or by corresponding with us by post, phone, email or otherwise.

Automated technologies or interactions. As you interact with our website, we may automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other similar technologies. [We may also receive Technical Data about you if you visit other websites employing our cookies. [Please see our **Cookie Policy** for further details].

How we use your personal data

We will only use your personal data when we have a legitimate basis for doing so and will process it in a fair and lawful way for limited purposes. Most commonly, we will use your personal data in the following circumstances:

- Where we need to comply with a legal or regulatory obligation and the Council is under a legal duty, for example collecting Council Tax.
- Where it is necessary to perform our Public Task in order to deliver public services (or those of a third party where there is a data sharing agreement) and your interests and fundamental rights do not override those interests.
- Where we are involved in a contract and processing is required, for example a contract of employment or a contract to provide services.
- Where a persons vital interests are at stake and the Council must carry out the activity to protect them from harm.
- Where it is entirely optional and consent is given freely in respect of the processing of your information, for example you have asked to be kept up-to-date with a public consultation.
- To prevent and detect fraud and other crimes
- To plan, monitor, and improve service performance
- Legal proceedings, including prosecutions by the Council
- To ensure our records are up to date and accurate

Marketing

Generally we do not rely on consent as a legal basis for processing your personal data other than in relation to sending third party direct marketing communications where you have agreed to this. You have the right to withdraw consent to marketing at any time by contacting us.

We only do limited marketing where you have signed up to receive it; usually through emails, bulletins or brochures and you can choose to unsubscribe at any time.

We do not sell any of our data to third parties.

Unsubscribe

Where you unsubscribe from receiving marketing messages, this will not apply to personal data provided to us as a result of provision of statutory services to you.

Data security

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We have put in place procedures to deal with any suspected personal data breach and will notify you and the ICO of a breach where we are legally required to do so.

Data retention

How long will you use my personal data for?

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, accounting, or reporting requirements.

Each department will have its own separate policy.

Data sharing

We often enter into data sharing agreements with third parties who deliver public services on our behalf under these agreements we may share your information with the third party in performance of our public task, we will only share your information when it is completely necessary to do so and only the minimum information will be shared.

Instead of entering into specific data sharing agreements some are done via the **Surrey Multi-Agency Information Sharing Protocol (MAISP)** which provides a common understanding for all the agencies in Surrey to work to and is recommended for use where there is no context-specific protocol – all members of **MAISP** are bound by its principles. More information on the MAISO can be found on the Surrey County Council website.

Sharing information about individuals between public authorities is often essential if we need to keep people safe, or ensure they get the best services. This sharing must only happen when it is legal and necessary to do so and adequate safeguards are in place to protect the security of the information.

The Council will / may share your information within the Council to ensure that all our records about you are accurate, or where there is a necessity for different departments to provide a service to you.

For more information on how the different services within the Council may share your information please look at the individual service privacy notice.

Vulnerable Persons Data

The Council has a statutory requirement to collect, use and share vulnerable adult data under the Civil Contingencies Act 2004, the act places a duty on authorities to "maintain plans for the purpose of ensuring that if an emergency occurs or is likely to occur it is able to perform its function so far as necessary for the purpose of preventing, reducing, controlling or mitigating its effects". As part of this planning we may share vulnerable adults data with other Surrey Local Resilience Forum partners (e.g. emergency services, local authorities, health trusts, voluntary organisations/charities, utility companies, transport companies, government agencies) to facilitate planning, facilitate response and recovery during incidents, and other activities in relation to Civil Contingencies work. We will only share this

data where there is a legal basis, ensuring that adequate safeguards are in place and only the minimum information is shared.

Prevention of fraud and crime

We also collect, use and share Personal Data internally and to other bodies responsible for auditing and administering public funds, or where undertaking a public function in order to detect fraud and protect public funds. For example, we participate in the Cabinet Office's National Fraud Initiative which compares computer records, usually personal information, to locate data differences as these may indicate potentially fraudulent claims and payments.

Further details on where we may share you information can be found in the privacy policy of the specific departments within the Council available on request.

Transferring data outside of the EEA

The Council does not share data with organisations outside of the UK and European Economic Area (EEA), however the Council is moving some of its IT systems to cloud based solutions, this could mean that a cloud server may be housed outside of the UK or EEA. Data must not be transferred to a Country or territory outside the UK or EEA unless that Country or Territory protects the rights and freedoms of Data Subjects. Where the Council uses cloud based IT solutions it will always complete a Data Privacy Impact Assessment (DPIA) to identify exactly where the data is being stored and only when we are completely satisfied that the location meets the standards and contracts are in place, will we adopt the service.

Your legal rights

You have the right to:

- Request access to your personal data (commonly known as a "data subject access request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.

  You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive.

- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you, if applicable, at

the time of your request and in order to assist us in carrying out this function we need as much information as possible to identify you and to identify the data you are specifically referring to.

- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:

  (a) if you want us to establish the data's accuracy;
  (b) where our use of the data is unlawful but you do not want us to erase it;
  (c) where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
  (d) you have objected to our use of your data but we need to verify whether we have overriding legitimate grounds to use it.

- Request the transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you.

- Withdraw consent at any time where we are relying on consent to process your personal data. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

To submit a 'your rights' request please email **data.protection@surreyheath.gov.uk** or call the Data Protection team on 01276 707632.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

Time limit to respond

All legitimate requests should receive a response within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.