PRIVACY AND DATA PROTECTION POLICY

Document history

Date	Version	Author	Changes made
17 February 2017	Draft 4.1	Geraldine Sharman	Initial revision of 2015 policy
20 February 2017	Draft 4.2	Geraldine Sharman	Reviewed and written policy
16 March 2017	Version 4	Geraldine Sharman	Approved version

Approvals

Name	Role/Title	Date
Janet Jones	ICT Manager	23rd February 2017
Louise Livingston	Executive Head of Transformation	
Kelvin Menon	Executive Head of Finance as Senior Information Risk Owner	3rd March 2017
Belinda Tam/Jenny Villamayor	Interim HR Manager	1st March 2017
CMT members		3rd March 2017
Joint Staff Consultative Group		16th March 2017

Document Filename and Location:

Filename:170217 Data Protection Policy (v4)

Format	Version	Filepath	Owner
Draft	Draft 4.1	G:\Information Rights\Data Protection\Data Protection Policy\Data Protection Policy 2017	Geraldine Sharman
Published	Version	G:\Information Rights\Data Protection\Data Protection Policy\Data Protection Policy 2017	4th May 2017

Scope of this policy statement

1.1 Surrey Heath Borough Council is committed to fulfilling its obligations under the Data Protection Act 1998 and the Privacy and Electronic Communication Regulations 2003 and has produced this policy to provide assurance to customers and to assist officers.

1.2 This document is one of a group of policies which are linked together to cover all aspects of Information Management and Security and is subject to ongoing review in the light of changes in the law and the Information Commissioner's guidance. This version of the Data Protection Policy is an update of a previous version issued in July 2015.

1.3 The Data Protection Act 1998 establishes a framework of rights and duties which are designed to safeguard personal data. This framework balances the legitimate needs of organisations 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 for the privacy of their personal details. These include members of the public, clients and customers, current, past and prospective employees, suppliers (such as sole traders) and other individuals with whom the Council communicates. These people are called "data subjects".

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

1.5 Personal data under the Data Protection Act 1998 is information about a living individual who can be identified from the information. The information can be factual information (e.g. names and addresses) or expressions of opinion or intentions about an individual.

1.6 Surrey Heath 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, electronically or recorded on other material such as audio, visual media (CCTV) or Body Worn Cameras.

1.7 Surrey Heath 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 the Council treats personal information lawfully and correctly and respects privacy.

1.8 To this end, Surrey Heath Borough Council fully endorses and adheres to the principles of Data Protection, as set out in Schedule 1 of the Data Protection Act 1998 (See Section 3).

1.9 The Information Commissioner's Office has a number of regulatory actions it can take under the Privacy and Electronic Regulations. This includes issuing a Monetary Penalty Notice, requiring an organisation to pay up to £500,000 for serious breaches

1.10 On the 25th May 2018 the Data Protection Act 1998 will be replaced by the General Data Protection Regulation (GDPR). In order to implement the GDPR Surrey Heath will need to commit to the review of the GDPR and implement any changes required.

1.11 In addition, Surrey Heath Borough Council will ensure in order to comply with the Data Protection Act 1998 that:

- there is an officer with specific responsibility for data protection in the organisation. The Nominated Person is the Information Governance Manager
- every legal person (including companies who act as Data Processors) managing and handling personal information understand that they are contractually responsible for following good data protection practice
- every person managing and handling personal information is appropriately trained to do so
- every person managing and handling personal information is appropriately supervised
- anyone wanting to make enquiries about handling personal information, whether a member of staff, councillor 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
- people whose information is being collected will know why and for what purpose their information is being collected and that it will not be used for any other purpose than that stated to them when they give it. This is unless it is required by law, to prevent and detect fraud or to protect the individual.

2 Roles and Responsibilities

2.1 All staff will ensure that:

- they understand how this policy works
- assess the kind of information they use whilst carrying out their work and whether they have responsibility for any personal information
- make sure that they use personal information in accordance with this policy and the eight data protection principles for which they are personally liable

- they complete any mandatory Data Protection training required

- the follow the Data Protection Policy, otherwise disciplinary action may be taken against any Borough Council employee who breaches any instruction contained in, or following from, the Data Protection Act. Compliance with the Data Protection Act forms part of Staff Terms and Conditions.

2.2 Senior Information Risk Owner (Senior Information Risk Owner)

- the Local Government Data Handling Guidelines, which covers handling personal data, requires that all Local Authorities have a board member who acts as a SIRO. Within Surrey Heath, the Executive Head of Finance acts as the SIRO.

- the SIRO will work with the Data Protection Officer to implement any changes to the Data Protection Act including the implementation of the General Data Protection Regulation.

2.3 Executive Heads/Heads of Service will:

- ensure compliance with the Data Protection Act 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

- ensure Privacy Impact Assessments, in relation to each new project or proposal are completed, that will involve the use of personal information or affect privacy. This must be carried out at the beginning and any review of the project. The Information Governance Manager must be informed and involved at an early stage

- ensure staff complete any mandatory training

- Under the GDPR there are a number of changes which will affect contracts and new projects. It is therefore important that if any new projects are being considered then Data Protection needs to be built in at the beginning (Privacy by Design). Contracts will need to reflect the changes; including any Data Processors will have the same liability as the Data Controller.

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

- Baseline personnel checks at recruitment

- to ensure that new members of staff are made aware of this policy document at induction stage as all staff are covered by Staff Terms and Conditions

- to ensure that new starters and temporary staff who require training complete the first available Information Governance training course after their start date. Information Governance training is held quarterly

2.5 The Information Governance Manager will:

- Act as the Data Protection Officer under the direction of the Senior Information Risk Owner until the introduction of the General Data Protection Regulation
- 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 the notification of the Council's processing to the Information Commissioner
- ensure that appropriate compliance monitoring is carried out in conjunction with the Senior Information Risk Owner
- complete subject access requests (which should be made in writing using the Council's pro forma request, if possible). Enquiries about Data Protection should be addressed to the Information Governance Manager
- keep up to date with changes in the law and guidance on the Data Protection Act and the General Data Protection Regulation.
- advise and write as required Data Sharing Agreements
- advise and ensure data sharing is compliant with the Data Protection Act including S29(3) requests
- Produce a project plan for implementing the GDPR and manage the introduction

3 Data Protection Principles

3.1 The Act applies to any processing of personal information. Processing includes virtually anything that can be applied to information, including acquisition, storage and destruction as well as active use. This includes CCTV images, photographs and digital images.

3.2 The eight principles of personal information are:

1. Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met

2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

4. Personal data shall be accurate and, where necessary, kept up to date

5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes

6. Personal data shall be processed in accordance with the rights of data subjects under this Act

7. Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data

8. Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

More detailed explanations of the principles can be found on the Information Commissioner's website
http://www.ico.org.uk/for_organisations/data_protection/the_guide

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

- they respect their data protection rights
- all electronic and manual filing systems conform to the eight Data Protection Principles

4 Surrey Heath Borough Council's commitment to Data Protection

4.1 Surrey Heath Borough Council is a Data Controller as defined in the Data Protection Act and is registered with the Information Commissioner's Office

4.2 Surrey Heath Borough Council is committed to whole-hearted compliance with the Data Protection Act 1998. The Council will carry out the following:

- 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

- check and maintain the quality of information used

- 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.

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

- 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 the Information Security Policy and subsidiary policies

- not disclose personal data, either within or outside the organisation, to any unauthorised recipient. Manage breaches in line with the Data Security Breach Management Policy and Procedure

- ensure that personal information is not transferred abroad, including storing information in the Cloud, without suitable safeguards. Discussions will take place with the Data Protection Officer before transferring any information overseas

5 Data Subject Access

5.1 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), 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 within 40 working days of a Subject Access Request being received together with the statutory fee of £10 and proof of identity. Where the Council is unable to process the request within the timeframe, the data subject should 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.

5.2 Any queries regarding Data Protection, or any requests for personal information whether from the person themselves or from a third party must be referred to the Data Protection Officer.

6 Data Sharing and Data Matching

6.1 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
- promote the prevention and detection of fraud and crime
- the Courts under direction of a Court Order

6.2 Appropriate information sharing protocols must be in place before personal information will be shared with other agencies. These protocols will be reviewed, amended and updated on a regular basis. They must comply with the Information Commissioner's Data Sharing Code. Surrey Heath Borough Council is a signatory of the Surrey Multi Agency Information Sharing Policy (MAISP). Any information shared with signatories of MAISP must comply with this. A list of the signatories can be found on the Surrey County Council website

6.3 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.

7 Contractual and partnership arrangements

7.1 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'.

7.2 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.

7.3 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. The responsibilities of each data controller should be expressly and clearly laid out.

8 Training

8.1 Data Protection training is mandatory for all employees of the Council. All new employees will attend one of the regular Information Governance courses run by the Information Governance Manager. Annually, all employees will complete the Data Protection e-learning package.

8.2 All staff will be required to attend training for the General Data Protection Regulation during 2017/18.

9 General Data Protection Regulation

9.1 Many of the GDPR's main concepts and principles are the same as those in the current Data Protection Act. However, there are new elements and significant changes which will require things to be done differently. A new Data Protection Policy will need to be produced for the new Regulation. This policy highlights some of the major changes and work which needs to be carried out to implement the GDPR.

9.2 "Personal data" is more detailed than in the Data Protection Act, for example online identifiers (IP addresses) can be personal detail. This is to provide for a wide range of personal identifiers to constitute personal data, reflecting changes in technology and the way organisations collect information about people.

9.3 Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

9.4 Key changes include:

- The current system of Notification to the ICO will be replaced by a requirement for Data Controllers to keep an internal record in relation to all personal data they process
- Consent - similar to the current Data Protection Act but pre-ticked boxes (opt out) or inactivity will no longer constitute consent
- Data Subject Rights – "Right to be Forgotten" means that data subjects will be able to request their personal data is erased by the Data Controller. This is not an absolute. The fee for making a subject access request will no longer apply and the time to respond will reduce from 40 calendar days to one month.
- Breaches – currently there is no legal obligation to report personal breaches. Under the new regulation that as soon as the Data Controller becomes aware that a personal breach has occurred it must report to the ICO within 72 hours and also notify the Data Subjects.
- Fines – there will be two different levels of fines, one up to 20 million Euros (e.g. failing to comply with Data Subjects' rights or the conditions for processing) or 10 million Euros (e.g. failing to keep records or complying with security obligations

- Data Protection Officer – this will be a statutory role. The Council will need to appoint someone within the Council. They must be someone with expert knowledge of data protection law. They will need to inform and advise, monitor compliance and manage internal data protection activities and be the first point of contact with the Information Commissioner's Office. The DPO must report to the board level, operate independently and is not dismissed or penalised for performing their task, have adequate resources to enable DPO's to meet their GDPR obligations.

- Data Portability – a person shall be able to transfer their personal data from one electronic processing system to and into another in a structured and commonly used electronic format.

9.5 The work to be carried out to implement the General Data Protection Regulation will follow the 12 steps highlighted in the Information Commissioner's checklist.

- Awareness
- Information you hold
- Communicating privacy information
- Individuals rights
- Subject access requests
- Legal basis for processing personal data
- Consent
- Children
- Data breaches
- Data Protection by Design and Data Protection Impact Assessments
- Data Protection Officer
- International

10 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
- Whistleblowing

- 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

11 Review

11.1 This policy will be reviewed in 2018 to comply with the General Data Protection Regulation which comes into force on 25th May 2018.

Geraldine Sharman
Information Governance Manager
February 2017