Data Protection Policy

1. Summary

This policy sets out how the council will comply with the General Data Protection Regulation (GDPR), Data Protection Act 2018, other regulations and good practice standards to protect the personal information of everyone who receives services from, or provides services to, the council, and includes the rights of staff and councillors. It informs people of their rights, and suppliers of their responsibilities.

2. Scope

This policy applies to all employees, contractors, agency staff and councillors. It covers the personal data we collect and use on paper and electronically. It covers our corporate databases, computer network and archive of paper records. It covers video and photographs, voice recordings, CCTV and mobile devices such as laptops, mobile phones, memory sticks and pendant alarms.

3. Accountability

The *council* is a data controller which means that it decides why and how personal data is processed and is accountable for its handling of personal information.

The *Senior Information Risk Officer* (SIRO) is the Director of Corporate Services who is accountable for protecting the council's information assets.

The *Caldicott Guardian* is the Director of Community and Housing. The Caldicott Guardian is responsible for protecting the confidentiality of people's health and social care information and making sure it is used properly.

The *Information Governance Board* is chaired by the SIRO and includes the Heads of Information Governance; IT Service Delivery; IT Systems; and Human Resources; Caldicott Guardian; Legal and departmental IG Champions. The Board is responsible for providing strategic guidance and regular updates to the SIRO and Caldicott Guardian for the management of the council's information assets.

The *Data Protection Officer* is a position required in law to ensure the council complies with data protection legislation and acts as a single point of contact for individuals who want to find out about their data. The Assistant Director of Corporate Governance is the council's Data Protection Officer.

Each *employee and supplier* is bound by a contractual duty of confidentiality.

The council is registered with the *Information Commissioner's Office (ICO)*, the independent regulator of compliance with data protection legislation.

The council maintains a *register of processing activities (ROPA)* of the personal information we are responsible for.

4. Personal data

We generally refer to a person or individual in this policy, although the term in law is ‘data subject’.

Processing data means any operation performed on personal data, whether using a computer or manual filing systems. It includes collection, use, recording, storing, sending and deleting personal data.

In this policy, personal data means any information relating to an identifiable living person. This means they can be identified from information such as a name, an address, an identification number (e.g. National Insurance number, NHS number or case reference number), location data, etc.

Special categories of personal data are known as personal sensitive data. This is data regarding an individual’s racial or ethnic origin, political opinion, religious or philosophical belief, trade union membership, genetic data and biometric data (fingerprints, eye scans etc.) for the purpose of uniquely identifying a person, data concerning health or data concerning a person’s sex life or sexual orientation.

As special categories of personal data are more sensitive, there are extra safeguards in place to ensure the safe use and sharing of this information.

5. Data protection principles

The council applies the six data protection principles in its processing of personal data:

- Processed lawfully, fairly and in a transparent way.
- Collected for a specific purpose.
- Adequate, relevant and limited to what’s necessary.
- Kept up to date.
- Kept for only as long as necessary.
- Protected with appropriate security.

6. Data protection is a fundamental right

The protection of a person’s data is a fundamental right. Under the Human Rights Act 1998, everyone has the right to respect for their private and family life, their home and their correspondence. This includes respect for an individual’s private and confidential information, particularly when storing and sharing data. This right can be limited in certain circumstances but any limitation must balance the competing interests of an individual and of the community as a whole.

We will only process a person’s data in accordance with data protection legislation.

7. Lawful basis of processing personal data

There are different lawful reasons for processing personal data and special categories of personal data. The council always uses at least one lawful basis for processing personal information and at least one lawful basis for processing special categories of personal data.

The six lawful reasons for processing personal data are:

a) **Consent** – An individual has given consent for the processing of their personal data;

b) **Contract** – The council has a contract with a person and need to process their personal data to comply with our obligations under the contract; or we haven't yet got a contract but have been asked to do something as a first step (e.g. provide a quote) and we need to process the personal data to do what they ask;

c) **Legal obligation** – The council is obliged to process personal data to comply with a legal obligation;

d) **Vital interests** – The processing of personal data is necessary to protect someone's life (vital interests);

e) **Public task** – The processing of personal data is necessary under public functions and powers set out in law; or the council needs to perform a specific task in the public interest;

f) **Legitimate interests** – The processing of personal data is in the legitimate interests of the council, where we use an individual's data in ways that people would reasonably expect and that have a minimal privacy impact.

The lawful bases for processing special categories of data are:

(a) an individual has given explicit consent to the processing of personal data for one or more specified purposes, except where limited by law;

(b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the council or a person under employment, social security and social protection law or a collective agreement under law;

(c) processing is necessary to protect the vital interests of a person or where the person is physically or legally incapable of giving consent;

(d) processing by non-for-profit bodies for legitimate activities with appropriate safeguards;

(e) processing relates to personal data which have been made public by a person;

(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;

(g) processing is necessary for reasons of substantial public interest under law;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of law or pursuant to contract with a health professional and subject to the duty of confidentiality;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, subject to the duty of confidentiality;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

8. Consent

Where the council relies on consent or explicit consent as the lawful basis for processing, we ensure that it is made clear to individuals how to give consent and how the council will then use their information.

We will keep evidence of consent (who, when, how and what we told people) and have procedures in place to make it easy for this consent to be withdrawn at a later date. Once this has been done, the council will cease processing this information.

For explicit consent we will ensure the individual provides a very clear and specific statement of consent.

The council will not rely on consent as the legal basis for processing information for services it delivers as part of its statutory duties or public functions as a local authority.

9. Duty of confidentiality

Our staff and councillors abide by a common law duty of confidentiality. This means that personal information that has been given to a member of staff or a councillor by an individual should not be used or disclosed further, except as originally given by that individual, or with their permission.

Our staff and councillors are subject to a Code of Conduct which includes maintaining confidentiality and all staff have a confidentiality clause in their contracts.

Our social care professionals are subject to their professional codes of conduct relating to the confidentiality of their relationship with service users and clients.

10. Information about criminal offences

The processing of information about criminal allegations, convictions or offences by the council is in accordance with our legal obligations and because we have legal authority in certain areas, such as the enforcement of parking rules, preventing fly tipping, upholding food hygiene and licensing of pubs and clubs. Further details can be found in the council's Law Enforcement Policy.

11. Surveillance

The council operates CCTV for traffic management and public safety, in line with the ICOs Code of Practice.

The council uses the Regulation of Investigatory Powers Act 2000 (RIPA) in line with the Investigatory Powers Commissioner's Codes of Practice, to conduct covert surveillance, including directed surveillance or the use of a covert human intelligence source. The council's Standards Committee receives a six monthly report and monitors the use of such powers.

12. Children

The council applies particular protection to the collecting and processing of children's personal data because they may be less aware of the risks involved.

Where we offer an online service, which is not a preventive or counselling service directly to a child, only children aged 13 or over are able to provide their own consent. For children under this age, we obtain consent from whoever holds parental responsibility for the child.

13. Automated processing

Where the council relies on automated decision-making (making a decision solely by automated means without any human involvement) we inform the affected individuals via our privacy notices and allow them an opportunity to challenge any decisions directly with a member of council staff.

14. How we handle personal information - Privacy Notices

The council provides privacy notices, which are statements about the collection and use of individual's personal data. The information includes our purposes for processing the personal data, retention periods for that personal data, and who it will be shared with. The council has a specific children-friendly Privacy Notice.

This information is on the council's website, and individuals are referred to it at the time we collect their personal data from them.

15. Individual Rights

Individuals whose data is processed by the council have a number of rights in law.

(a) **Access** – The council will respond to a subject access request by an individual for access to the information we hold about them. There is no charge for this service. We will respond within one month. We may take longer than one month and up to three months if the request is complicated. If extra time is required we will inform the individual of this prior to the deadline for a response.

(b) **Rectification** – The council will respond within one month to a request from an individual to have inaccurate personal data rectified (corrected), or completed if it is incomplete. Where the council can lawfully refuse to rectify the data, we will explain why.

(c) **Erasure** – The council will respond within one month to a request from an individual to have personal data erased. Where the council can lawfully refuse to erase the data, we will explain why.

(d) **Restrict processing** – The council will consider a request from an individual asking to restrict the processing of their personal data in the following circumstances:

- An individual has contested the accuracy of the information and is waiting for us to respond or change the information;
- An individual has objected to the processing and we are considering whether we have a legitimate reason to process the information;
- The processing is unlawful but the individual concerned would prefer the council to restrict the data rather than erase it;
- The council no longer needs the data but the individual requires it to establish, exercise or defend a legal claim.

(e) **Data Portability** – The council will respond within one month to a request from an individual to move, copy or transfer personal data from the council's computer network to another in a safe and secure way. We will do this in a structured, commonly used and machine readable form and free of charge.

(f) **Object** – The council will consider a request from an individual objecting to the processing of their personal data in relation to:

- processing based on legitimate interests or the performance of a task in the public interest/exercise of official authority (including profiling);
- direct marketing (including profiling); and
- processing for purposes of scientific/historical research and statistics.

16. Information sharing

The council is committed to providing efficient, easy to access services that meet the needs of individuals. To achieve these aims it is important that we share information across the council and with other organisations effectively. When we share personal information we will do so securely and in compliance with our information security policy.

We will work with our partners to develop frameworks and formal information sharing agreements to help facilitate the regular bulk sharing of information with internal teams and external stakeholders. These agreements will detail what information is shared, how it will be shared and the retention period for this information.

If information is shared with other services, this will be explained in the relevant privacy notice. It may also be shared, where necessary, with other organisations that provide services on our behalf, such as providers of residential accommodation.

We will always seek to share information with partners in accordance with the Caldicott principles and for the benefit of service users. We will also share information when we are legally required to do so i.e. in response to a court order or a police request.

The information is only shared if it is relevant and limited to what is necessary for the purpose for which it has been requested. We will inform individuals about who their data is shared with in our privacy notices.

Personal information may also be provided to central government departments, where we are required to do so by law or, under certain circumstances, to other local authorities to support the provision of services for residents who move between boroughs. Information may also be provided for statistical research, although this will not include names and addresses unless we have been given permission to provide that information. Information is shared with the Police, Customs and Excise, the Inland Revenue and the National Fraud Initiative to prevent and detect crime, prosecute offenders and assess taxes.

We expect our officers to respect the confidentiality of information about individuals. Whilst we will support officers in taking decisions about information sharing in accordance with their professional judgement, we may take disciplinary or legal action against officers who use personal data for unauthorised purposes.

17. Transfers to other countries

Most of our processing occurs in the UK or European Economic Area (EEA) where there are common standards for the processing of personal data. If the council ever has to transfer personal data outside of the UK or the EEA, there will be checks in place to ensure adequate data protection arrangements of that country.

18. Privacy by design

The council is committed to a privacy by design approach and have built in processes to ensure privacy is considered at the outset of any procurement of new IT systems or any major projects; changes; or development to existing services.

19. Data Protection Impact Assessments

The council requires all its services to carry out Data Protection Impact Assessments when they introduce new technology or significant changes to the processing of personal data. The assessment identifies the risk to customers' privacy and what steps can be taken to reduce this where possible, whilst providing a service to the customer. They will be revised and updated whenever necessary.

20. Contractors

Where the council has a contractual relationship with another organisation or individual, we will ensure we are clear about the contractor's role, responsibilities and accountability in relation to personal information through the use of standardised contract clauses.

21. Pseudonymisation and Anonymisation

Pseudonymisation is a procedure by which the most identifying fields within an information asset are replaced by one or more artificial identifiers, or pseudonyms. There can be a single pseudonym for a collection of replaced fields or a pseudonym per replaced field.

Anonymisation is the process of removing identifying particulars or details from an information asset which can then safely be used for statistical or other purposes.

The council is committed to using pseudonymised or anonymised information as much as is practical, and this will be the default position in the following areas:

- service planning to better understand the needs of Merton residents and to provide the services requested;
- helping us to build up a picture of how we are performing at delivering services to residents and what services the people of Merton need;
- analysis of costs and spend of services we provide so that we can ensure better and efficient use of public funds;
- evaluating, monitoring health of the Merton population and protecting and improving public health.

22. Information Security

The council has an Information Security policy detailing the technical and organisational measures to protect personal data, including annual mandatory information security training for all council staff.

The council obtains independent assurance of its information security and complies with the information security standards of the Public Service Network.

The council complies with the Data Security and Protection Toolkit of the Department of Health / NHS for handling personal confidential data.

23. Breaches

The council has in place appropriate systems and processes to reduce the likelihood of information breaches occurring. If a breach does occur, it is reported to the Information Governance Team who undertake an immediate investigation and risk assessment. Data breaches are discussed on a quarterly basis at the Information Governance Board and at departmental management team meetings. Where a breach is a serious risk to the rights and freedoms of anyone, it will be reported to the Information Commissioner within 72 hours.

Lessons are learned from breaches and where necessary, processes and / or systems are changed and bespoke training is provided to staff. Weekly bulletins are sent to staff to remind them of their obligations through the data security tip of the week.

24. Data Protection Officer

The council has appointed a Data Protection Officer who is responsible for ensuring organisation compliance with data protection legislation. The Data Protection Officer and the Information Governance Team can be contacted at: data.protection@merton.gov.uk

25. How to complain

If you think we have misused or not looked after your personal data properly, you can complain. Your complaint will be investigated by the Information Governance Team and they will respond within one month, giving details of how to escalate your complaint to the ICO if you are still not satisfied.

26. Misuse of personal information

It is an offence for a person, knowingly or recklessly, without the consent of the council to:

- obtain or disclose personal data or the information contained in personal data, or
- procure the disclosure to another person of the information contained in personal data.

Unless the disclosure

- was necessary to prevent or detect crime; or
- was required or authorised by law.

The council will take action against anyone found to be supplying information to a third party or using information for their own purposes without the consent of the council, or a reasonable belief that they were working in accordance with the wishes of the council. Such offences are criminal offences and may be punished with a fine or imprisonment.