MENDIP DISTRICT COUNCIL

LAW AND GOVERNACE / INFORMATION GOVERNANCE

DATA PROTECTION POLICY

Author: James Ellis
Document Name: Data Protection Policy
Document Number:
Effective Date: 22/07/2022
Date due for review: 22/07/2024
Responsible for review: Data Protection Officer

Version control

Number	Effective Date	Author / Reviewer	Comments (e.g. details of any policies being replaced)
1	01/11/2019	James Ellis	Draft
1.1	10/12/2019	David Clark	Comments on draft
1.2	06/01/2020	James Ellis	Final Draft
1.3	06/07/2020	James Ellis	Final
2	01/07/2022	James Ellis	Updated for terminology

Dissemination

Name or Team	Method	Date	Version
Staff	My Mendip	10/07/2020	1.3
CMT	Email – for approval	11/07/2022	2

Publication of current version

Location	Date of Publication
MDC Website	26/07/2022

Approvals for current version

Name	Date of Approval
Data Protection Officer	06/01/2020
Group Manager Law and Governance	06/01/2020
Scrutiny Policy and Strategy Working Group	21/02/2020
CMT	06/07/2020
CMT	22/07/2022

Contents

1. Introduction

1.1 Mendip District Council (the council) supports the objectives of the UK General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 (DPA) and is committed to ensuring compliance with the data protection legislation.

1.2 Mendip District Council is a Data Controller under the UK GDPR, and is registered as such with the Information Commissioners Office.

1.3 The processing of personal and 'special category' personal data by the council is essential to delivering the services and functions of the council, and the council always seeks to do so in a fair, lawful and transparent manner and in compliance with the Principles of UK GDPR.

1.4 The UK GDPR and the Human Rights Act (HRA) 1998 set out that the processing of personal data must respect the fundamental rights and freedoms of data subjects (individuals), including the right to privacy, while at the same time ensuring the processing is adequate enough for council services to function effectively.

1.5 This policy sets out at a high level how the council works towards complying with the UK GDPR and DPA and should be read alongside the council's Information Rights Policy, Freedom of Information Policy, Access to Information Charging Policy, Privacy Policy and service level privacy notices.

2. Purpose and Scope

2.1 The purpose of this policy is to ensure that the provisions of the UK GDPR and DPA are adhered to and that the council works to uphold the rights and privacy of data subjects**,** ensuring that their personal data is processed in line with the Principles and obligations of the regulations.

2.2 This policy extends to all personal data being processed by the council. Where personal data is being processed on the council's behalf, by Data Processors and Sub Processors, the council will take reasonable steps to ensure that these Principles and objectives are upheld.

2.3 In particular this policy will:

- Assist the council to comply with all requirements of the UK GDPR and DPA and to communicate to data subjects how this is achieved
- Ensure that personal data is processed fairly, lawfully and transparently and with the appropriate technical and organisational measures in place to keep it safe and secure
- Show how the council works towards the requirements in UK GDPR for

increased privacy through data processing, such as 'Privacy by Design and by Default'

- Ensure that personal data is readily available on request and that information rights requests from data subjects are dealt with correctly and in a timely manner.

- Ensure adequate consideration is given to whether or not personal information should be disclosed, particularly in respect of requests from third parties and when sharing data between Data Controllers

- Increase awareness among data subjects in respect of how their personal data is processed and stored by the council

- Ensure that the council has in place the correct processes to handle breaches of compliance with the regulations, such as personal data security breaches.

2.4 The council is committed to promoting greater openness and to providing increased transparency of data processing through building public trust and confidence in the way that the council manage the personal data of our citizens, staff and customers.

3. Aims

3.1 This policy sets out the councils' commitment to upholding the data protection principles set out in the UK GDPR and to fulfilling our obligations and responsibilities as a Data Controller. It seeks to strike an appropriate balance between the councils need to make use of personal data while maintaining respect for the privacy of individuals, and to provide a useful guide to the public on the council responsibilities with regard to the processing of their personal data.

3.2 This policy is also designed to assist council staff and elected members, and our Data Processors, to meet their statutory obligations under the UK GDPR and DPA.

4. Council Statement on Data Protection Requirements

4.1 Mendip District Council is committed to fulfilling our obligations and responsibilities as a Data Controller under data protection law and to ensuring that data subjects individual rights and freedoms are protected. This is achieved in the following ways:

- The council will comply with Article 8 of the HRA in respect of the processing of personal data.

- The council is committed to the fair, lawful and transparent processing of personal data.

- The council will only process personal data and ‘special category’ data where it has a lawful basis to do so (the council is a public body and in the vast majority of cases is acting under statute of an Act of Parliament, or some other official authority or legal obligation).

- The council, as the Data Controller, will make individuals aware of the lawful basis and the purpose(s) for the processing of their personal data in a privacy notice published on the council website or otherwise appropriately communicated to data subjects.

- Where consent is the lawful basis, the consent will be compliant with UK GDPR and will be taken to mean a freely given, specific, informed and unambiguous indication of the data subject’s wishes by which they, through a specific statement or by a clear affirmative action, signify their agreement to the processing of personal data relating to them.

- All personal data that the council holds will be processed in accordance with the six principles of the UK GDPR and in line with the information given in the council’s privacy notices.

- The council will provide general information to the public about their statutory rights under the UK GDPR and DPA and is committed to complying with any statutory timescales for processing requests made under the regulations. This is set out in the councils Information Rights Policy on our website.

- The council will process the minimum amount of personal data necessary to carry out our functions, and every effort will be made to ensure the accuracy and relevance of the data being processed.

- The council will maintain all electronic and manual records in accordance with the principle to keep personal data only for as long as necessary, with a relevant retention period being set according to our retention policy and communicated to data subjects in a privacy notice.

- Periodic risk assessments will be undertaken, via audit reviews, and when inadequate controls are identified, appropriate technical and organisational measures will be taken to address the issues, in line with the level of risk identified.

- Personal data will only be used for the direct promotion or marketing of services by the council with the affirmative consent of an individual or, when directly linked to a relevant council service, with another appropriate lawful basis in place. The council will not normally undertake indirect marketing to

data subjects of any kind.

- Data Processing by third parties on behalf of the council will only be carried out under an appropriate legally binding contract.

- Data sharing and data matching with external agencies, such as other public bodies and central government, will only be carried out when required by law or under an appropriate data sharing protocol or agreement.

- All staff and elected members will be trained to an appropriate level in cyber security and the safe handling of personal data.

- Breaches of this policy may be subject to action under the council's disciplinary procedure and councillor code of conduct.

4.2 All personal data will be processed by the council in line with the six Data Protection Principles of UK GDPR.

As detailed below, personal data will be:

- **Processed fairly, lawfully and in a transparent manner.** The council achieves this by ensuring that it identifies a clear reason for undertaking the processing, normally under statute, and identifies and records the lawful basis. This information is then published on the council website in a privacy notice.

- **Collected for a specific, identified and legitimate purposes and not further processed in a manner that is incompatible with those purposes.** This is known in UK GDPR as the 'purposed limitation' principle. The council achieves this by identifying a clear purpose for the processing, where required meeting the condition of being 'necessary' to achieving the stated purpose, and notifying data subjects of the purpose in a privacy notice.

- **Adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.** This is known in UK GDPR as the 'data minimisation' principle. The council achieves this by only collecting what is necessary and considering the data minimisation principle at all steps of the data journey.

- **Accurate and, where necessary, kept up to date.** This is known in UK GDPR as the 'accuracy' principle. The council achieves this by training staff in the need to ensure the accuracy of data and through services identifying what data needs to be kept up to date, and reviewing this on a regular basis.

- **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.** This is known in UK GDPR as the 'storage limitation' principle. The council achieves this by identifying a retention period for all data and ensures that data is securely deleted or disposed of at the end of this period.

This information is then published on the council website in a privacy notice.

- **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.** This is known in UK GDPR as the 'integrity and confidentiality' principle. The council achieves this by having appropriate controls in place to access council systems, by maintaining secure networks, up to date system patching and virus detection, and ensuring sensitive information is locked away. The council also maintain a clear desk policy and regularly train staff on how to identify and deal with data breaches, should they occur.

- **The council will ensure that it keeps records of processing and evidence of its compliance with the principles under the data protection legislation.** This is known in UK GDPR as the 'accountability' principle. The council achieve this by appointing a Data Protection Officer to coordinate compliance across the council and by keeping records of processing.

5. Governance, Roles and Responsibilities

5.1 The council's **Corporate Management Team (CMT)** is responsible for approving this policy and for managing compliance with the UK GDPR and DPA, in direct consultation with the Data Protection Officer and the Head of Service for Law and Governance.

5.2 The council's **Data Protection Officer (DPO)** is responsible for the provision of advice, guidance and training regarding data protection legislation and is responsible for keeping this document up to date. This includes supporting the council with Data Protection Impact Assessments (DPIAs) and reporting directly to CMT on a regular basis on compliance with the data protection regulations.

5.3 **Heads of Service** are information asset owners for their service groups and are responsible for ensuring day to day operational compliance with this policy within their own departments, including ensuring that staff in their groups complete the necessary training, and for becoming involved in consultations with the Data Protection Officer when applicable.

5.4 **Audit Committee** will ensure oversight by receiving regular information on Cyber Security and Data Protection risk and compliance as part of the quarterly Strategic Risk Register report.

5.5 **All employees** of the council are responsible for processing personal data in line with data protection principles and for ensuring that Subject Access Requests, and other information rights requests, are dealt with in accordance with this policy. This includes ensuring that personal data is handled safely and

securely and that any security breaches are reported through the correct channels without delay.

5.6 **Internal Audit** will undertake audits to assess the data protection procedures and policies in place and report their recommendations to council management and Audit Committee, appropriate to the risks identified.

6. Information Rights in UK GDPR

6.1 Requests from data subjects for copies of personal data that the council hold about them (Subject Access Requests) can be made in writing or verbally. This includes requests transmitted by electronic means, providing they are received in a legible form and are capable of being used to communicate with the data subject.

6.2 If a person is unable to articulate their request in writing we will provide advice to assist them in formulating their request.

6.3 The council will normally respond to the request in the same manner in which the request is received, taking into account necessary security requirements based on the sensitivity of the data. This means that requests made electronically (i.e. by the website or email) will be routinely responded to by email.

6.4 The council will take reasonable steps to validate the identity of the requestor, which will not exceed those checks normally undertaken by services to identify individuals, but which may require the requestor to provide photographic and/or official documentation as evidence of identity to the council.

6.5 If the information sought is not described in a way that would enable the council to identify and locate the requested material, for example because the scope of the request is not defined or the timescale covered by the request is not specified, the council will seek additional clarification. This will happen as soon as possible after receiving the initial request and will set out what information the council requires from the data subject in order to proceed with the request.

6.6 The council will normally only deal with information requests from the data subject themselves, unless it is confirmed that the requestor has the authorisation of the data subject to make the request on their behalf (e.g. a solicitor or other legal advocate).

6.7 The council will not normally make any charges for complying with Subject Access Requests.

6.8 The council also receives information requests for personal data from other

public bodies, legal representatives and law enforcement agencies. This will often happen without the knowledge of the data subject. Personal data will only be provided in instances where a valid request has been made from a qualifying organisation, citing an appropriate exemption under the DPA which the council is satisfied has been reasonably met. For more information see the section below on Exemptions.

6.9 All requests for personal data made by the data subject will be dealt with under the UK GDPR, not the Freedom of Information Act 2000.

6.10 The individual Data Subjects Rights are set out in the council's Information Rights Policy on our website. Subject to some legal exceptions, UK GDPR gives individuals the rights set out below in respect of their personal data.

- The right to request a copy of any information we hold about you.
- The right to rectification (if inaccurate data is held).
- The right to erasure ('right to be forgotten'), in certain circumstances.
- The right to restrict processing, in certain circumstances.
- The right to data portability (personal data transferred from one data controller to another), in certain circumstances.
- The right to object to direct marketing and to other data processing, in certain circumstances.
- The right to be informed of, and to object to, automated decision making and profiling, where this has been no human intervention.

6.11 With the exception of the right of access, these rights under UK GDPR are not absolute and different rights apply to different lawful bases of processing. The table below from the ICO website shows which rights apply based upon the lawful basis of processing (a cross denotes that a right does not apply):

	Right to erasure	Right to portability	Right to object
Consent			✖ but right to withdraw consent
Contract			✖
Legal obligation	✖	✖	✖
Vital interests		✖	✖
Public task	✖	✖	
Legitimate interests		✖	

7. Responding to Information Rights Requests

7.1 The council is committed to dealing with requests for information promptly and no later than the statutory timeframe of one calendar month.

7.2 Requests will be acknowledged by the council, at which point requestors will be advised of the date by which to expect a response.

7.3 The council would not expect every application for information to take one calendar month and will endeavour, where possible, to provide the requested information at the earliest opportunity. If the request does require proof of identity, then the council will only consider it has a valid request once proof of identity has been received.

7.4 If the council consider the request to be complex, the deadline can be extended by up to two calendar months. In this instance the council will notify the applicant in writing within one month that the request requires further time and will provide an estimate of a ‘reasonable time’ by which they expect a response to be made.

7.5 These estimates shall be realistic and reasonable taking into account the circumstances of each particular case.

7.6 The council will generally respond to requests in the manner in which the request was made, but will normally take steps to try and provide copies of personal data electronically, unless otherwise agreed with the data subject.

7.7 The council will publish statistics quarterly to show its performance with these timeframes in the Corporate Performance Report.

8. Refusal of Information Rights Requests

8.1 The council will not supply information to a data subject if:

- We are not satisfied with the identity of the data subject
- Compliance with the request will inadvertently disclose personal information relating to another individual without their consent
- The applicant has recently requested the same or similar information

8.2 In certain circumstances, the council may find that a request from a data subject is 'manifestly unfounded or excessive', in which case the request can be refused or a reasonable charge made to complete the request. In these cases, the data subject will be notified of the reasons, and any potential charges, in writing within one month of making a valid request.

8.3 When the council does refuse a request or withhold certain information, an explanation will be provided including details of how the applicant can complain about the council's decision to the ICO.

9. Exempting Information from Non-Disclosure under the DPA

9.1 The UK GDPR is designed to prevent access by third parties to a data subject's personal data. However, under the DPA there are circumstances which allow disclosure of a data subject's personal data to a third party, or for it to be used in a situation that would normally be considered to be a breach of the UK GDPR.

9.2 Examples of exemptions from the non-disclosure of personal data are given below. This list is not exhaustive.

- Crime and taxation: general

    a) the prevention and detection of crime
    b) the apprehension or prosecution of offenders, or
    c) the assessment or collection of any tax or duty or of any imposition of a similar nature

- Crime and taxation: Risk Assessment
- Immigration

- Information required to be disclosed by law or in connection with legal proceedings
- Legal professional privilege
- Functions designed to protect the public

9.3 The council will only facilitate the use of these exemptions where it is satisfied that it is appropriate to do so, i.e. prevention of crime, or where a third party has a legal requirement to locate an individual to collect taxation

9.4 In certain cases these exemptions remove other rights normally applied under UK GDPR, such as the right to notified and certain specific principles of UK GDPR, in so far as they are incompatible with the purpose of applying the exemption. For example, the council will not notify a data subject of the personal data released under a valid exemption request from the Police investigating a crime, nor will the council provide a copy of the police request under a Subject Access Request (SAR), because to do so would prejudice the aim of the request.

10. Data Processors and Sub Processors

10.1 The council is committed to fulfilling its obligations and responsibilities as a Data Controller under UK GDPR and DPA, and this extends to ensuring that our Data Processors, who are jointly responsible for UK GDPR compliance, understand the requirements and ensure they comply with the regulations.

10.2 The council uses a number of third parties to provide services on our behalf, and where personal data is processed in this way the council uses an appropriate mechanism, such as a binding contract or Data Processing Agreement, to set out what is required to ensure secure and compliant data processing.

10.3 These agreements include; clauses that the Data Processor will only process personal data under the direct instruction of the council (as the Data Controller); what the purpose and lawful basis for the processing is and what security measures should be in place, and the requirement to notify the data controller that a data subject has made an information rights request.

10.4 This requirement extends to sub processors, who must also ensure compliance and can only be employed with the agreement of the Data Controller.

11. Data Protection by Design and Default

11.1 UK GDPR requires that Data Controllers and Data Processors move towards

a position of default data protection compliance by designing in UK GDPR compliance to all new data processing, and by improving existing processing through identifying weaknesses through regular audits. Data protection by design is about considering data protection and privacy issues upfront and hard wiring it into everything you do.

11.2 One key way in which the council achieves this is by screening all new data processing for privacy risk, using the ICO Data Protection Impact Assessment (DPIA) framework, which is mandatory under UK GDPR for all high risk processing. Where a DPIA is required, the DPO will work with the service to identify the risks, if any, and reduce or eliminate them through appropriate controls and mitigation. Where a high risk remains the council will consult with the ICO and will not proceed with processing until reaching a satisfactory resolution.

11.3 All DPIAs undergo an approval process, in which the DPO will make a recommendation on the risks and appropriate controls, which will be assessed and signed off by the relevant Information Asset Owner, normally a Head of Service or their agreed delegate.

11.4 Where appropriate, DPIAs will be reviewed and kept up to date.

11.5 A record of DPIAs undertaken will be retained to assist the council in working towards compliance with the accountability principle.

12. Complaints

12.1 Where a data subject is unhappy about the way that the council has processed their personal data, they are entitled to complain about the actions of the council under the Right to Object. This can done by contacting the Data Protection Officer. All complaints should be forwarded to:

Data Protection Officer
Mendip District Council
Cannards Grave Road
Shepton Mallet
Somerset
BA4 5BT

E-mail : DPO@mendip.gov.uk

12.2 The applicant will receive a response to their query or complaint as soon as possible, and in any event within one month in line with the Right to Object under UK GDPR. If the applicant remains dissatisfied with the councils reply, they have the option of taking their complaint to the Information Commissioner (at the address below) who will investigate the issue and come to a decision.

Information Commissioner's Office
Wycliffe House,
Water Lane
Wilmslow
Cheshire SK9 5AF

Email: casework@ico.org.uk

Appropriate Policy Document for Mendip District Council

The Data Protection Act 2018 (DPA 2018) outlines the requirement for an Appropriate Policy Document (APD) to be in place when processing special category (SC) and criminal offence (CO) data under certain specified conditions.

Almost all of the substantial public interest conditions in Schedule 1 Part 2 of the DPA 2018, plus the condition for processing employment, social security and social protection data, require you to have an APD in place. (See Schedule 1 paragraphs 1(1)(b) and 5).

This document should demonstrate that the processing of SC and CO data based on these specific Schedule 1 conditions is compliant with the requirements of the General Data Protection Regulation (GDPR) Article 5 principles. In particular, it should outline your retention policies with respect to this data. (See Schedule 1 Part 4).

If you process SC or CO data for a number of different purposes you do not need a separate policy document for each condition or processing activity – one document can cover them all. You may reference policies and procedures which are relevant to all the identified processing. Whilst you may explain your compliance with the principles in general terms, without specific reference to each individual Schedule 1 condition you have listed, you should provide the data subject with sufficient information to understand how you are processing their SC or CO data and how long you will retain it for.

However if you rely on one of these conditions, your general record of processing activities under GDPR Article 30 must include:

(a) the condition which is relied upon;
(b) how the processing satisfies Article 6 of the GDPR (lawfulness of processing); and

(c) whether the personal data is retained and erased in accordance with the retention policies outlined in this APD, and if not,

the reasons why these policies have not been followed.

The APD therefore complements your general record of processing under Article 30 of the GDPR and provides SC and CO data with further protection and accountability. See Schedule 1 Part 4 paragraph 41.

You must keep the APD under review and will need to retain it until six months after the date you stop the relevant processing. If the Commissioner asks to see it, you must provide it free of charge. See Schedule 1 Part 4 paragraph 40.

You should read this document alongside our Guide to the GDPR.

Note your APD does not have to be structured in accordance with this document. This template

is intended as a guideline only.

Description of data processed

Give a brief description of each category of SC/CO data processed. You may wish to refer to your Article 30 record of processing for that particular data:

Racial or ethnic origin data
Political opinions data
Religious or philosophical beliefs data
Trade union membership data
Health data
Sex life and sexual orientation data

Schedule 1 condition for processing

Give the name and paragraph number of your relevant Schedule 1 condition(s) for processing. Alternatively, you may wish to provide a link to your privacy policy, your record of processing or any other relevant documentation:

Special category data is processed under the following Article 9 conditions and the associated DPA Schedule 1 conditions:

(b) Employment, social security and social protection law

- checking if individuals are entitled to work in the UK
- ensuring the health, safety and welfare of employees
- maintaining records of statutory sick pay and maternity pay
- deducting trade union subscriptions from payroll

In respect of social security (benefits) and other statutory functions:

- sickness
- maternity and paternity
- invalidity or disability
- old-age
- death and survivorship
- accidents at work or occupational diseases
- unemployment
- housing
- family life and children
- other forms of social exclusion

(f) Legal claims and judicial acts

- actual or prospective court proceedings
- obtaining legal advice
- establishing, exercising or defending legal rights in any other way

(g) Substantial public interest

- statutory and government purposes
- equality of opportunity or treatment
- racial and ethnic diversity at senior levels
- preventing or detecting unlawful acts
- protecting the public
- regulatory requirements
- preventing fraud
- safeguarding of children and individuals at risk
- safeguarding of economic well-being of certain individuals
- occupational pensions
- elected representatives responding to requests
- disclosure to elected representatives

(h) Health or social care

- preventive or occupational medicine
- the assessment of an employee's working capacity

Procedures for ensuring compliance with the principles

You need to explain, in brief and with reference to the conditions relied upon, how your procedures ensure your compliance with the principles below.

This helps you meet your accountability obligations. You have a responsibility to demonstrate that your policies and procedures ensure your compliance with the wider requirements of the UK GDPR and in particular the principles. The sensitivity of SC and CO data means the technical and organisational measures you have in place to protect such data are crucially important.

The questions listed in each box are intended to help you describe how you satisfy each principle generally, and are based on the checklist for each principle provided in the Guide to the GDPR. They are not exhaustive and are only intended to act as a guideline.

In explaining your compliance with the principles you should consider the specifics of your processing with respect to the SC and CO data you have identified above.
You may also wish to answer other questions which are included in our Guide to the GDPR checklists (see links in each section below).

There is also no requirement to reproduce information which is recorded elsewhere – **questions may be answered with a link or reference to other documentation, to your policies and procedures, Data Protection Impact Assessments (DPIAs) or to your privacy notices.**

Accountability principle
We maintain appropriate documentation of our processing activities We have in place an appropriate data protection policy We carry out data protection impact assessments (DPIA) for uses of personal data that are likely to result in high risk to individuals' rights and freedoms We train staff and elected members regularly in cyber security, information governance and safe data handling and keep records of training completion
Principle (a): lawfulness, fairness and transparency
We identified an appropriate lawful basis for processing and a further Schedule 1 condition for processing all SC/CO data. We make appropriate privacy information available with respect to the SC/CO data in service level privacy notices on our website. We open and honest when we collect the SC/CO data and we ensure we do not deceive or mislead people about its use.
Principle (b): purpose limitation
We clearly identify our purpose(s) for processing the SC/CO data We included appropriate details of these purposes in our privacy information for individuals in service level privacy notices on our website. If we plan to use personal data for a new purpose (other than a legal obligation or function set out in law), we check that this is compatible with our original purpose or get specific consent for the new purpose
Principle (c): data minimisation
We only collect SC/CO personal data we actually need for our specified purposes and we train staff to understand and follow this policy We are satisfied that we have sufficient SC/CO data to properly fulfil those purposes We take reasonable steps to periodically review this particular SC/CO data, and delete anything we don't need
Principle (d): accuracy
We have appropriate processes in place to check the accuracy of the SC/CO data we collect. We have a process in place to identify when we need to keep the SC/CO data updated to properly fulfil our purpose, and we update it as necessary. We have of procedures which outline how we keep records of mistakes and opinions, how we deal with challenges to the accuracy of data and how we ensure compliance with the individual's right to rectification.
Principle (e): storage limitation
We carefully consider how long we keep the SC/CO data and can we justify this amount of time and publish it in service level privacy notices on our website.

We are working towards ensuring that all SC/CO data is deleted/securely destroyed according to its retention period
Principle (f): integrity and confidentiality (security)
We analyse the risks presented by our processing and use this to assess the appropriate level of security and organisational measures we need in place for the data. We are working towards an information security policy (or equivalent) regarding this SC/CO data and it will be regularly reviewed We are working towards putting other technical measures or controls in place because of the circumstances and the type of SC/CO data we are processing

Retention and erasure policies

You need to explain your retention and erasure policies with respect to each category of SC/CO data (this could include a link to your retention policy if you have one). You need to explicitly indicate how long you are likely to retain each specific category of SC/CO data.

This is published in the service level privacy notices on the council website. As a general rule, the SC/SO data is required to comply with a regulatory requirement, so it is retained for the same period as the normal personal data associated with the individual, unless otherwise stated.

APD review date

This APD will be reviewed annually by the Data Protection Officer.

Appendix 2

Glossary of Terms

Personal data	Any information relating to an identified or identifiable living individual ('data subject')
Special category personal data	Personal data which identifies: • Racial or ethnic origin • Political opinions • Religious/philosophical beliefs • Trade union • Processing of biometric/genetic data to identify someone • Health • Sex life or sexual orientation
Data Subject	A natural, living individual who can identified, directly or indirectly (sometimes referred to as an 'identifiable living individual'). Natural in this context means a person rather than a company or other legal entity
Processing	In relation to personal data, this means any operation or set of operations performed on personal data, such as: • Collection, recording, organisation, structuring, storage • Adaptation or alteration • Retrieval, consultation, use • Disclosure by sharing, dissemination, publication or otherwise making available • Alignment or combination, or • Restriction, erasure or destruction.
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data Processor	The natural or legal person, public authority, agency or other body which processes personal data on behalf of, and under the instruction of, the data controller
Lawful Basis	Refers to the lawful basis set out in UK GDPR, without which personal data must not be processed. These are:

	• Consent: the individual has given clear consent for you to process their personal data for a specific purpose. • Contract: the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract. • Legal obligation: the processing is necessary for you to comply with the law (not including contractual obligations). • Vital interests: the processing is necessary to protect someone's life. • Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law. • Legitimate interests: the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks.)
Condition for processing special categories of data	Similar to the lawful basis, in order to process 'special category data' an additional condition for processing is required. These are: • Explicit consent • Employment, social security and social protection (if authorised by law) • Vital interests • Not-for-profit bodies • Made public by the data subject • Legal claims or judicial acts • Reasons of substantial public interest (with a basis in law) • Health or social care (with a basis in law) • Public health (with a basis in law) • Archiving, research and statistics (with a basis in law)