ISPS-011

MID SUSSEX DISTRICT COUNCIL

Information Security Policy Suite

Data Protection Policy

November 2025

Data Protection Policy

1. Purpose

The purpose of this policy is to ensure appropriate measures are applied to comply with the six principles of the Data Protection Act 2018 ('the Act'), the General Data Protection Regulation (GDPR) and to meet the Councils' statutory requirements under these.

2. Scope

This policy applies to all staff, members, contractors and any other persons who have access to the Council's information, information systems and networks.

This policy applies to all information held, created, modified or accessed from the effective date of this policy. It includes information in any form, no matter whether it is stationary (e.g. an electronic or paper document) or in transit (e.g. file transfer, e-mail, fax, phone, post, courier). It also covers the buildings, premises and systems which contain that information.

3. Policy Statement

The policy of the Council is to ensure that it takes appropriate technical and organisational security measures that require that personal information is:

1. processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions are met within Schedule 9 and for sensitive personal data, Schedule 10
2. the data purpose shall be specific, explicit and legitimate and it must not be processed in a manner that is incompatible for the purpose for which it was collected
3. adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. accurate and where necessary, kept up to date
5. not be kept for longer than is necessary for that purpose or those purposes
6. processed in a manner that includes taking appropriate security measures as regards risks that arise form processing personal data

3.1 Data Subject Access Requests (DSAR)

All Data Subject Access Requests for information made to the Council under the Data Protection Act 2018 will be dealt with by the designated officers, and in accordance with the Council's Data Protection Code of Practice.

Access will be afforded in accordance with the Act to data subjects applying for such information in the specified manner. The Council has 30 calendar days in which to respond to a request. Under the Data (Use and Access) Act, the Council is only expected to undertake reasonable and proportionate searches when responding to DSAR's. The one month response time can now also be paused under the 'stop the clock' rule while awaiting identity verification or clarification from the requestor.

4. Responsibilities

This section should be read in conjunction with the responsibilities detailed in section 6 of the Information Governance and Security Policy. Additional responsibilities arising from this policy are specified below.

4.1 Data Protection Officer

Their responsibilities include:

- The maintenance of the Council's compliance
- annual renewal of notification registration
- dissemination of data protection information within the authority
- dealing with changes and modifications arising from legislation or codes of practice

4.1.1 Senior Managers

Are responsible for promoting and overseeing practices which comply with this policy, and for ensuring that managers, officers and Members are trained to carry out their responsibilities.

4.1.2 Managers

It is the responsibility of Managers to ensure compliance with this policy within their own service areas. Their responsibility includes:

- ensuring that staff are aware of their responsibilities under the Data Protection Act and the GDPR
- ensuring employees, including contractors, consultants and volunteers employed to undertake Council business follow the data protection policy and procedures
- ensure appropriate resources are in place to enable compliance with the data protection policy

In addition, it is the responsibility of Heads of Service to ensure that any new computerised or manual systems are compliant with the Data Protection Act and the GDPR and that they

notify the designated officer of any known future developments likely to affect registration.

4.1.3 All Staff

All staff must be aware of the Data Protection Act and the GDPR, and of their obligations under it.

Individual staff members may be personally liable for breaches of the Act if they act outside the authority of the data controller.

All new members of staff will be required to sign a non-disclosure document and will receive information about the Council's Data Protection Policy and procedures as part of their Induction Process and in training sessions provided by the Authority. Refresher training will be carried out for all staff on a regular basis, in particular when there are any changes in legislation, when there is an information security incident or on a three yearly cycle at the discretion of each authority.

4.1.4 Members

All elected Members are to be made fully aware of this policy and of their duties and responsibilities under the Act.

When Members handle personal information in their role as politicians or in their role as elected members, they are covered by their party or the Council's notification. As such, they have to handle personal information in line with the requirements of the Council's Data Protection Policy.

If Members use (process) personal information in their constituency work, or are independent elected Members, they will have to notify with the Information Commissioner's Office as a data controller in their own right.

5. Training associated with this Policy

This policy will be included in the Information Security suite of awareness materials and training courses and delivered with reference to the Training Guidelines.

If anyone requires support, advice or guidance on any element outlined in this policy they should speak with their line manager.

6. Monitoring

Compliance monitoring will be carried out by the Council's Information Security Manager (ISM) and through the Council's management structure.

6.1 Non-conformance

Disciplinary action in accordance with procedures approved by the Council may be taken against any employee who breaches the requirements of this policy.

6.2 Review

This Policy Template {Update field in Doc Properties} will initially be reviewed after 12 months and on a three yearly basis thereafter, unless there is a change in legislation which necessitates an earlier review.

7. Related documents

This policy should be read in conjunction with the following documents:

- Information Governance and Security Policy;
- Data Protection procedures
- Other policies in the Information Security Policy Suite.

8. Version Control

Author	Sheila Harris
Version 0.20	April 2023
Signed off by:	Simon Jones
Date of sign off:	April 2023
Review date:	November 2025
Next Review date:	November 2027