Data Protection Policy

Date approved	Cabinet 23.05.2018
Date of last review	Head of Policy and Governance Assistant Director Legal and Governance Information Governance Team Leader March 2025
Date of next review	16.08.2026

Contents

1. Purpose and objectives

1.1. This policy forms part of Shropshire Council's commitment to the safeguarding of personal data processed by its staff. Processing has a very broad definition, and includes activities such as creating, storing, consulting, amending, disclosing and destroying data. Shropshire Council processes the personal data of living individuals such as its staff, customers and contractors and partner organisations.

1.2. The objective of this policy is to ensure the Council:

- Complies with Data Protection legislation
- Processes personal information in accordance with the Data Protection Principles
- Supports the rights of data subjects
- Is able to work with partner organisations and providers when sharing data with them.

1.3. The Shropshire Plan 2022-2025 sets out the following commitment:

Using emerging technologies and digital solutions will enable us to provide our customers with improved and quicker access to information. We will data, feedback from our communities and best practice to provide intelligence and insights to inform our decision making, and monitor Outcomes to continually review what we do to ensure that our services benefit people and communities.

2. Introduction

Role	Responsible officer
Senior Information Risk Owner (SIRO)	Executive Director (Section 151)
Data Protection Officer	Information Governance Team Leader
Information Governance Lead	Head of Policy and Governance
Monitoring Officer	Service Director – Legal and Governance

2.1 As Shropshire Council is a public authority, it has a legal duty to appoint a designated Data Protection Officer. The Data Protection Officer has legal duties that they must fulfil including:

- Inform and advise the Council of its obligations in respect to data protection
- Monitor compliance with data protection legislation including awareness raising and training of staff
- Provide advice on data protection impact assessments
- Act as the first point of contact for the Information Commissioners Office

The Council's current designated Data Protection Officer is the Information Governance Team Leader. Contact can be made: Information.request@shropshire.gov.uk

3. The Council's Responsibilities

3.1. The Council maintains strict safeguards and controls by having:

- A Senior Information Risk Owner (SIRO) responsible for information risk within the authority.
- An Information Governance Team responsible for gathering and distributing information and issues relating to Data Protection and Data Privacy and other related legislation.
- Information Asset Owner's responsible for appropriate and full use and protection of information assets.
- Technical and organisational safeguards and controls in place to support information security and compliance with the requirements of Data Protection legislation.
- Contracts and service level agreements (SLA) between the Council and external organisations contain requirements relating to compliance with DPA 2018 legislation and is logged onto our contracts registered and is monitored.
- A requirement that all staff are receive annual awareness training so they can handle personal data appropriately and in line with this policy.

4. Responsibilities of staff and management

4.1. **The Council will ensure that all Council staff:**

- Fully understand their data protection obligations
- Check that any data processing activities they are dealing with comply with this policy and are justified.
- Don't use data in any unlawful way.
- Don't store data incorrectly, be careless with it or otherwise cause the Council to breach data protection laws and its policies.
- Comply with this policy at all times.
- Raise any concerns, notify any breaches or errors, and report anything suspicious or contradictory to this policy or the Council's legal obligations without delay by contacting information.request@shropshire,gov.uk .

4.2. **Line Managers are responsible for:**

- Ensuring that this policy is communicated to all employees, including temporary staff, contractors, agents and partners working for or on behalf of the Council.
- Ensuring that it is adhered to at all times.
- Ensuring that this policy is communicated to all elected members.
- Ensuring all employees complete the mandatory Data Protection and Cyber Security Awareness training when they start employment and refresh it annually.
- Ensuring that any request for information they receive is dealt with in line
- with the requirements of the DPA 2018.
- Ensuring that all elected members, contractors, agents and partners working for or on behalf of the Council complete the mandatory Data Protection and Cyber Security Awareness training.

5. Legislation, guidance and standards

5.1. The Council has an obligation to make sure that all information systems and processes meet the terms of all relevant legislation and contractual requirements, including the:

- Data Protection Act 2018
- The Protection of Freedoms Act 2012
- The Human Rights Act 1998
- Privacy and Electronic Communications Regulations 2000
- E-Privacy Regulation 2018
- Regulation of Investigatory Powers Act 2000
- Indecent display (Control) Act 1981
- Obscene Publications Act 1984
- Copyright, Designs and Patents Act 1988
- Theft Act 1978Common Law Duty of Confidentiality
- Equality Act 2010
- Terrorism Act 2006
- Limitation Act 1980
- The Caldicott Principles
- Copyright, Designs and Patents Act 1988
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Government Security Classification Scheme

6. The principles relating to the processing of personal data

6.1. Shropshire Council shall comply with the principles as outlined in Article 5 of the UK GDPR - A guide to the data protection principles | ICO. All staff must adhere to and comply with these principles at all times when processing any personal data as part of their work.

7. Special Category Data

7.1. Special Category data create more significant risks to a person's fundamental rights and freedoms and as such the DPA 2018 imposes stricter conditions on the processing of such data.

7.2. In cases where such data is being processed it needs more protection There are a separate set of conditions, one of which must be satisfied before this type of is processed.

8. Criminal Offence Data

8.1. Under the DPA 2018 there are specific rules regarding the processing of personal data relating to criminal convictions and offences[4]. Such data shall be carried out only under the control of "official authority" or when the processing is authorised by law providing for appropriate safeguards for the rights and freedoms of data subjects. The principles in section 5 of this policy will also apply to this data. Even where the Council has a condition for processing

offence data, it can only keep a comprehensive register of criminal convictions if it is doing so in an official capacity.

9. Accountability and transparency

9.1. All employees of Shropshire Council must ensure accountability and transparency in their use of personal data. Information Asset owners[5] are responsible for keeping a written record within the Council's Information Asset Register of how all the data processing activities comply with each of these Principles. The system must be kept up to date and anything added must be approved by the Council's Information Governance Team.

9.2. To comply with data protection laws and the accountability and transparency Principle of UK DPA 2018 2018, the Council must be able to demonstrate compliance. Officers are responsible for understanding their responsibilities to ensure the Council meets the following data protection obligations to:

- Fully implement all appropriate technical and organisational measures
- Maintain up to date and relevant documentation on all processing activities through the completion of the information Asset Register
- Ensure data sharing agreements are in place when sharing personal data with third party organisations
- Requirement for completion of Data Protection Impact Assessments prior to any work that might impact the personal information of data subjects
- Data minimisation by default
- Ensuring data is accurate and up to date
- Ensuring service area's corporate privacy notice covers any sharing they do
- to provide transparency.

10. Processing data fairly and lawfully

10.1. When processing any personal data, the information asset owner is required to ensure that there is a sufficient legal basis to do so as required under the DPA 2018. It is the asset owner's responsibility to check the lawful basis for processing or sharing any personal data being processed and make sure this is clearly recorded on the information asset system.

10.2. When making an assessment of the relevant lawful basis, the information asset owner will establish that the processing is necessary.

10.3. Information Asset owners will document how they have considered which lawful basis best applies to each processing purpose, and fully justify these decisions.

11. Consent

11.1 The lawful basis of Consent to process personal data should only be relied on where there is not an alternative appropriate lawful basis, such as legal

obligation and public task. Under the DPA 2018, strict regulations affect how consent is obtained to use an individual's personal data. Under the DPA 2018 consent must be clear, informed and unambiguous and most importantly must be opt-in and provided by way of a clear and affirmative action. More details about the new consent requirements can be found on the ICO website[7]

11.2 In all cases, whether you have obtained the data subject's consent or not, you need to ensure that the use of personal data is permitted in principle by local government law. If in doubt, please seek advice from either the Information Governance Team or Legal Services.

12. Sharing information with third parties

12.1 Information Asset Owners will ensure that there is an Information Sharing or Information Processing Agreement in place when sharing personal information with third parties external to the council. There may be exceptions to this, such exceptions will be dependent on the relationship with the other party/parties

12.2 Staff should seek advice from the Information Governance Team on the exceptions. Full details of what is required, as well as agreement templates, can be found on the intranet.

12.3 Information Asset Owners must consult with the Information Governance Team, to agree any new Information Sharing or Information Processing Agreements. The Information Governance Team must be notified of agreements that are in place to ensure that

12.4 Information Asset Owners must also ensure that any sharing or processing is recorded on the Information Asset Register and referenced in the relevant privacy notice.

13. Privacy notices

13.1. Individuals whose data is being processed by the Council must be informed of the lawful basis for processing their data, as well as the intended purpose. This should be communicated via a privacy notice. The Council has an obligation to communicate privacy notice information regardless whether we have collected the data directly from the individual, or we have received the information from another source.

13.2. Information Asset Owners must ensure that privacy notices are in place and cover all aspects of how the data will be used and shared.

13.3. When collecting personal data face to face, or over the phone, all officers must inform individuals of their right to review the Council's privacy notices online or request a hard copy.

14. Accuracy of data

14.1. Information Asset Owners must ensure that any personal data we process is accurate adequate, relevant and not excessive, given the purpose for which it was obtained. Personal data will not be processed if it has been obtained for one purpose for any unconnected purpose unless the individual concerned has agreed to this or would otherwise reasonably expect this.

14.2. Individuals may ask that we correct inaccurate personal data relating to them. If an officer believes that information is inaccurate they should take steps to amend the information Any requests to rectify information must be promptly referred to the Information Governance Team: information.request@shropshire.gov.uk.

15. Information Security

15.1. All staff within the Council must ensure that they keep personal data secure and take measures to prevent accidental loss or destruction of the data. All staff should ensure when processing and storing personal data that they:

- Ensure data is stored on secure systems
- Ensure any personal information is transmitted using approved secure means when sharing externally to the Council
- Ensure information is only accessed by and available to certain people who need to see it

15.2. The Information Security Policy details all of the relevant information security obligations. All staff must comply with the information security policy.

16. Data breaches

16.1. Any breach of this policy or of data protection laws must be reported to the Information Governance Team as soon as practically possible and within 24 hours of becoming aware of the incident. This means as soon as we have become aware of a breach. This should be done using the information security incident reporting form

16.2. The Council has a legal obligation to investigate and report any serious data breaches to the ICO within 72 hours. In the event of an information security incident; all officers must comply with the information security policy and breach guidance.

17. Data Storage

17.1. Where personal data is stored it must be done securely and adhere to the following:

- In cases when data is stored on printed paper, it should be kept in a secure place where unauthorised personnel cannot access it

- Printed data should be shredded when it is no longer needed
- Data stored electronically should be protected by strong passwords that are changed regularly in line with the Password policy
- Data stored on removable media such as CDs or memory sticks must be encrypted and locked away securely when they are not being used
- The Information Security Group must approve any cloud based storage solutions used to store personal data
- Servers containing personal data must be kept in a secure location, away from general office space
- All servers containing sensitive data must be approved and protected by security software
- Comply with the Information Security Policy

18. Data Retention

18.1. Personal data should only be retained for as long as is necessary for the purpose in which it was collected. The Council's Retention Schedule provides the statutory retention periods for the various types of information held. In the absence of a statutory retention period, Information Asset Owners should review the Council's retention schedule. Any adopted practices must be compliant and justifiable with the necessity principle imposed by data protection legislation.

19. Transferring data outside of the EEA

19.1. UK Data Protection Legislation contains rules about transfers of personal data to receivers located outside the UK. People's rights about their personal data must be protected or one of a limited number of exceptions must apply.

19.2. The transfer rules apply where the receiver is a separate controller or processor and legally distinct from the sender. The receiver can be a separate sole trader, partnership, company, public authority or other organisation, and includes separate companies in the same group.

19.3. The transfer rules do not apply where the receiver is an employee of the sender, or the sender and receiver are part of the same legal entity, such as a company. We refer to a transfer of personal data to these receivers located outside the UK as a 'restricted transfer'.

19.4. If we are considering transferring data to another country our Information Governance Team must be consulted in the first instance and they will advise on whether the transfer can take place.

20. Data Protection Impact Assessments (DPIA)

20.1. At the start of any project where the processing of personal data will be taking place, a DPIA should be considered. There are mandatory in cases where sensitive data is being processed or where a project involves new technology or some form of surveillance.

20.2. In cases where a DPIA is required this must be completed at the earliest stage of any project so that the risks are assessed at the outset. Once complete a

copy must then be sent to: information.request@shropshire.gov.uk so that we can advise and record the details of the assessment.

20.3. The screening questions at the start of Shropshire Council's DPIA will guide officers in their decision of whether the full DPIA is required. Additional guidance is made available on the Shropshire Council Intranet.

21. Rights of individuals

21.1. Under the DPA 2018 individuals have a number of rights in respect of the personal data we hold about them, the Council must ensure that individuals can exercise these rights. All Officers must recognise any of the following rights as statutory rights:

- Right to be informed – through privacy notices
- Right of access – enabling individuals to access their information through a subject access request (see section 21 for more details).
- Right to rectification – amending or rectifying personal data that is inaccurate or incomplete
- Right to erasure – deleting or removing an individual's data on request subject to certain exceptions
- Right to restrict processing – individuals' right to restrict, block or otherwise suppress the processing of their personal data.
- Right to data portability – individuals' right to have their data transferred or provided to them in a machine-readable format
- Right to object – individuals' right to object to their data being processed in certain circumstances
- Rights in relation to automated decision making and profiling

21.2. The Information Governance Team must be **notified within two working days** of any of the above statutory requests.

21.3. Not all data protection rights are absolute. Officers shouldn't agree to, or take any action, toward actioning requests without seeking advice from the Information Governance Team.

21.4. All service areas must assist the Information Governance Team on request when requiring information in order to comply with any such requests. Departments will promptly provide any information or guidance required and within five working days. All Officers must comply with the data protection rights procedure; further detail can be found on the Intranet.

22. Subject Access Requests

22.1. Individuals have a right to access any personal information the Council holds about them subject to certain exemptions. Such a request can be received electronically, by letter or over the phone and must be complied with within one month.

22.2. The relevant team receiving the request should refer it to the Information Governance Team in the first instance who will then advise of the next steps.

Further details about the Subject Access Request process can be found on the Intranet

23. Authorised Users

23.1. Authorised users will only have access to personal information where it is essential to their duties. Authorised users should discuss with their line manager any instance where access rights require clarification. Access rights are not to be regarded as permanent and are subject to change at any time depending upon the nature of the duties being fulfilled by the authorised user.

23.2. Authorised users with access to personal information must be familiar with the requirements of the DPA 2018 and familiar with the content of this policy.

23.3. Authorised users will only record information about an individual which is relevant, and should be aware that they may be required to justify what has been written and be prepared for that information to be released as part of a subject access request.

23.4. Any authorised user who is found to have inappropriately divulged personal information will be subject to investigation under the Council's disciplinary policy, which may result in dismissal and possible legal action. Where the authorised user is a Councillor they will be subject to investigation under the Members Code of Conduct in Part 5 of the Constitution.

23.5. All authorised users must follow good practice as indicated by the DPA 2018 and any such codes of practice issued by the office of the Information Commissioner or the Council, when processing personal data.

23.6. User access will be reviewed by system owners on a regular basis in line with the Information Security Policy.

24. Direct Marketing

24.1. The Council will not participate in direct marketing practices in the absence of:

- Explicit consent from the data subject
- A legitimate interest reason – officers must conduct a balancing exercise before seeking to rely on a legitimate interest reason.

24.2. Even where legitimate interests or explicit consent has been established, all correspondence and the relevant webpages must include opt-out options.

24.3. All individuals must be given the opportunity to opt-in to receive material at the point of data collection.

24.4. The appropriate opt-in mechanisms must be put in place where third party marketing or advertising materials are distributed to named individuals. In situations where this cannot be feasibly done, the materials must not be distributed.

25. Elected Members

25.1. Elected members are likely to have three different roles:

- As a member of the council, for example, as a cabinet member or a member of a committee.
- A representative of residents of their division, for example, in dealing with complaints.
- They may represent a political party, particularly at election time.

25.2. The Council is the Data Controller for information generated and managed in the administration of Council business.

25.3. When acting as an elected representative, Elected members would be Data Controllers on their own behalf.

25.4. When acting on behalf of a political party, for instance as an office holder, elected members are entitled to rely upon the registration made by the party.

25.5. Elected members are bound by the terms of the DPA 2018 for the duration of their tenure of office. Elected members must, when their term of office expires or for some other reason they cease to be an elected member, arrange for the transfer or secure disposal of all personal information held by them or their support staff on their behalf.

25.6. Where information is being transferred, the Assistant Director Legal and Governance will be notified and make the necessary arrangements for the transfer and future management of the information transferred.

26. Compliance with the Data Protection Policy

26.1. The Data Protection Officer is responsible for monitoring compliance with this policy.

26.2. If employees knowingly do not comply with Council policies, procedures or guidelines, the Council may take appropriate action in accordance with the Employee Code of Conduct.

26.3. Use by Council members must at all times be in accordance with the standards and Code of Conduct for Council members.

27. Other Relevant Policies, Standards and Procedures

27.1. These can be found on the Intranet or contact the information Governance Team on: information.request@shropshire.gov.uk.

28. Contact Details

28.1. Please contact the information.request@shropshire.gov.uk with enquiries about this or any other referenced policy, procedure or law.

Email to: information.request@shropshire.gov.uk.
Telephone: 01743 252179

Appendix 1

Definitions

Personal data	'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Personal data we gather may include: individuals' phone number, email address, educational background, financial and pay details etc.*
Special categories of personal data	Special categories of data include information about an individual's racial or ethnic origin, political opinions, religious or similar beliefs, trade union membership (or non-membership), physical or mental health or condition, criminal offences, or related proceedings, and genetic and biometric information
Data controller	'Data controller' means 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; where the purposes and means of such processing are determined by law.
Data processor	'Processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Processing	'Processing' means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
Supervisory authority	This is the national body responsible for data protection. The supervisory authority for our organisation is the Information Commissioners Office.