# DATA PROTECTION POLICY

DOCUMENT CONTROL

| **Document Responsibility** | | |
|---|---|---|
| **Name** | **Title** | **Service** |
| Information Governance Team | Data Protection Policy | Legal, Democratic, Digital and Customer Services |

| **Change History** | | |
|---|---|---|
| **Version** | **Date** | **Comments** |
| 01.0 | October 2012 | Information Governance Officer |
| 02.0 | July 2019 | Major amendments to reflect GDPR and DPA 2018 |
| 02.1 | October 2019 | Minor amendments from Legal |
| 02.2 | 24 October 2019 | Minor amendments from CMT |
| 03.0 | April 2023 | Minor Changes (accessibility)<br>Amended to reflect legislative changes, operational practice, designations and contact information. |
| 03.1 | May 2023 | Minor corrections, for submission to May 2023 P&R Committee |
| | | |

| **Policy Review** | | | |
|---|---|---|---|
| **Updating Frequency** | **Review Date** | **Person Responsible** | **Service** |
| 3 years unless required earlier | April 2026 | Information Governance Team | Legal, Democratic, Digital and Customer Services |

| **Document Review & Approvals – this document requires the following approvals** | | | |
|---|---|---|---|
| **Name** | **Action** | **Date** | **Communication** |
| P&R Committee | Approved | 23 May 2023 | |

# Contents

## 1.0 Introduction and Policy Statement

1.1 Inverclyde Council ('the Council') collects and processes personal information about its customers, employees and others to allow the Council to carry out many of its functions and responsibilities. This personal information, however it is acquired, held, processed, released or destroyed, must be dealt with lawfully and appropriately in accordance with Data Protection Legislation.

1.2 Dealing appropriately with personal information will not only ensure that the Council complies with its legal obligations but will contribute to maintaining the confidence of customers, employees and others.

1.3 This Policy sets out the Council's commitment to ensuring that any Personal Data, including Special Category Personal Data, which the Council processes, is processed in compliance with Data Protection Legislation. The Council seeks to ensure that good data protection practice is embedded in the culture of the Council and its employees.

1.4 This Policy sets out appropriate guidance and safeguards to ensure compliance with Data Protection Legislation.

1.5 The Council will ensure that all employees who handle Personal Data on its behalf are made aware of their responsibilities under this Policy and other relevant data protection and information security policies and that adequate training and supervision is provided.

1.6 To comply with Data Protection Legislation, information about individuals must be:

- processed lawfully, fairly and in a transparent manner;
- collected for specified, explicit and legitimate purposes;
- adequate, relevant and not excessive;
- accurate and, where necessary, kept up to date;
- retained for no longer than is necessary; and
- stored safely and securely

The Council will inform individuals about the Processing that it undertakes, through privacy notices and direct contact, and will make it clear to individuals what is happening with and to their Personal Data.

## 2.0 Definitions

2.1 The following outlines the key definitions and technical terms that are used in this document:

**Data Controller:** Any person or organisation who decides how any personal information can be held and processed, and for what purposes. Inverclyde Council is a Data Controller. In addition, individual Elected Members can be Data Controllers.

**Data Processor:** Any person (other than a Council employee) or organisation (for example, contractors and agents) who process personal information on behalf of the Council.

**Data Protection Legislation:** legislation relating to data protection, the processing of Personal Data and privacy including (i) the Data Protection Act 2018 (ii) the UK GDPR and (iii) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended).

**Data Subject:** Any living individual in respect of whom the Council holds or processes Personal Data.

**Personal Data:** Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, identification number, location data including online identifiers including IP address. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

**Processing:** Any operation related to the holding, organisation, retrieval, disclosure and deletion of data and includes obtaining and recording data; accessing, altering, adding to, merging, deleting data; retrieval, consultation or use of data; disclosure or otherwise making available of data.

**Special Category Personal Data:** Different from Personal Data, relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sexual life or criminal convictions, biometric, genetic. This type of data is subject to much stricter conditions of processing.

**Subject Access Request**: A right of access by individuals to their Personal Data held by the Council.

**UK GDPR:** The UK General Data Protection Regulation.

## 3.0 Scope

3.1 This Policy applies to all employees and Elected Members of the Council. Any breach of Data Protection Legislation or this Policy may result in disciplinary action for an employee, referral of an Elected Member to the Standards Commission and may also constitute a criminal offence.

3.2 The Policy is applicable to all Personal Data held by the Council irrespective of whether the information is held or accessed on Council premises or accessed remotely via mobile or home working. Personal Data held on removable devices and other portable media is also covered by this Policy.

3.3 Other third parties, including but not limited to, agencies, consultants, contractors, volunteers, agents or any other individual Processing Personal Data on behalf of the Council, are required to comply with this Policy.

3.4 This Policy applies to all situations where the Council processes (collects, stores, uses, shares) Personal Data about living individuals. It includes information stored in any format including but not limited to Personal Data held:

- electronically;
- on paper;
- on CCTV;

- in photographs; and
- on audio equipment.

3.5 Appendix 1 sets out the Data Protection Principles ('the Key Principles') defined in the Data Protection Legislation.

## 4.0 Responsibilities

4.1 The Council is the Data Controller under Data Protection Legislation.

4.2 The Corporate Management Team, Chief Officers and Service Managers are responsible for ensuring their teams and employees are aware of this Policy and for developing and encouraging robust information handling practices.

4.3 Compliance with Data Protection Legislation is the responsibility of all employees and Elected Members who process personal information.

4.4 Each Service and its senior management will retain a service responsibility for compliance with the provisions of the Data Protection Legislation and this Policy.

4.5 All Services will nominate an officer whose role will be to:

- monitor compliance within their Service;
- pass on advice and training;
- maintain the accuracy of their Service's input into the Council's Information Asset Register (IAR) and;
- to ensure that Subject Access Requests are properly and timeously processed.

4.6 All employees will be responsible for following procedures and systems for maintaining appropriate security of the Personal Data to which they have access.

4.7 Employees are required to complete mandatory data protection and information security training provided by the Council's Inverclyde Learns platform. These modules can be completed as many times as necessary for refresher training.

4.8 Managers are responsible for ensuring that employees within their Service are trained appropriately.

4.9 From time to time, Services will monitor their compliance with the Council's policies, procedures and guidelines and review their security arrangements.

4.10 The Corporate Management Team will ensure that employees are provided with guidance, training and procedures to promote a culture of compliance with the Data Protection Legislation and with this Policy.

4.11 The Council's Data Protection work will be overseen by the Information Governance Steering Group (IGSG). The IGSG is currently led by the Council's Senior Information Risk Officer. Council Services have nominated representatives to raise and progress data protection issues with the group. The IGSG reports into the Corporate Management Team and also to relevant Council committees such as the Policy & Resources Committee.

4.12 The Council's Senior Information Risk Owner (SIRO) sits on the Corporate Management Team and has overall responsibility for Information Management and Information Risk Management within the Council.

The SIRO:

- Acts as an advocate for information risk at the Corporate Management Team;
- Drives culture change regarding information risks in a realistic and effective manner;
- Is consulted on matters arising from information incidents; and
- In liaison with the Chief Executive and Directors, ensures the Information Asset Owner and supporting roles within Services are in place to support the SIRO role.

The Council's SIRO is the Head of Legal, Democratic, Digital and Customer Services.

4.13 The Council's Data Protection Officer (DPO) has corporate responsibility to:

- Inform and advise the Council and its employees about their obligations to comply with the Data Protection Legislation and other data protection laws;
- Monitor compliance with Data Protection Legislation and other data protection laws, including the assignment of responsibilities, raising awareness, developing training, training employees involved in the Processing areas and working on audit related matters;
- Provide advice about Data Protection Impact Assessments (explained further in section 12) and monitor their performance;
- Co-operate with the supervisory authority (the Information Commissioner's Office); and;
- Act as a point of contact for the Information Commissioner's Office on issues related to the Processing of Personal Data.

The Council's DPO is Vicky Pollock who can be contacted at dataprotection@inverclyde.gov.uk.

4.14 In recognition of our Data Protection obligations and in addition to this policy, a range of policies, procedures and guidelines promoting compliance and best practice have been developed to support a robust data governance framework.

1. Acceptable Use of Information Systems Policy
2. Records Management Policy
3. The Policy for the Retention and Disposal of Documents and Records Paper and Electronic.
4. Code of Conduct for Employees
5. Information Sharing Protocol
6. Data Breach Management Protocol
7. Data Protection Impact Assessment Guidance
8. GDPR Employee Guide
9. Privacy Notice Guidance

This list is not exhaustive, and all relevant data protection and wider information management guidance can be located under the Information Governance section on the Council intranet.

## 5.0 Special Category Personal Data

5.1 The Council processes Special Category Personal Data of employees, service users and third parties as is necessary to carry out its many functions and responsibilities.

5.2 Special Category Personal Data is subject to much stricter conditions of Processing.

5.3 Appendix 2 sets out the Council's policy statement and additional safeguards on Processing Special Category Data and Personal Data relating to criminal convictions and offences.

## 6.0 Implementation of Key Principles

6.1 The Council must demonstrate that it complies with Data Protection Legislation by having appropriate policies and procedures in place by documenting the Personal Data it is processing, why it is processing and legal basis for doing so.

6.2 In complying with the key principles of the Data Protection Legislation set out in Appendix 1, the following practices will be applied:-

a) The Council will ensure that the legal basis for Processing Personal Data is identified in advance and that all Processing is in compliance with the Data Protection Legislation;

b) The Council will ensure that all sharing of Personal Data with other organisations will be appropriately documented;

c) When Personal Data is collected the Data Subject will be provided with a Privacy Notice, providing information about what the Council collects, why this information is needed and how it will be processed. Any exceptions to this will be documented;

d) The Council will identify and collect the minimum amount of information that is necessary for the purpose. If it becomes necessary to hold or obtain additional information about certain individuals, such information will only be collected and recorded in relation to those individuals;

e) The Council will adopt policies that ensure that all relevant information is kept accurate and up to date. Where the Council identifies an inaccuracy or a Data Subject indicates that information held by the Council or a business partner is inaccurate, the error will be rectified by the owner of the data;

f) The Council will implement procedures in relation to the retention and disposal of Personal Data in accordance with the Policy for Retention and Disposal of Records;

g) The Council has processes in place to ensure that requests made by an individual to exercise their rights under Data Protection Legislation can be facilitated;

h) The Council will ensure that appropriate security measures are in place so that Personal Data can only be accessed by those who need to access it and that it is held and transferred securely;

i) Personal Data will be appropriately safeguarded from accidental destruction, theft or any other loss; and

j) Where there is a requirement to take Personal Data off-site, procedures will be adopted to ensure the safe keeping of that data.

## 7.0 Disclosure of Data

7.1 The Council must ensure that Personal Data is not disclosed to unauthorised third parties. All employees and Elected Members must ensure there is a lawful basis to share Personal Data before disclosing to a third party. Personal Data can be disclosed where one of the following legal bases apply:

- The individual has given their explicit consent;
- Where the disclosure forms part of the Council's statutory task and where the Data Protection Act 2018 permits such disclosure without consent in relation to specific purposes;
- Where the Council is legally obliged to disclose data;
- Where disclosure of data is required in relation to a contract which the individual has entered into;
- If the sharing of information is necessary in the vital interests of the data subject.

## 8.0 Data Subject Rights

8.1 Data Subjects have the following rights regarding data Processing and the data that is recorded about them:

- Right to be informed;
- Right of access;
- Right to rectification of inaccurate data;
- Right to erasure in certain circumstances;
- Right to object to certain Processing, including the right to prevent Processing for direct marketing;
- Right to prevent automated decision-making;
- Right to data portability; and
- Right to claim compensation for damages caused by a data breach.

8.2 An individual has the right to access their own Personal Data and can do so by making a Subject Access Request.

8.3 The Council will ensure that the rights of Data Subjects are respected. Further information on compliance with all Data Subject rights can be sought by contacting the Information Governance Team.

## 9.0 Data Protection Fee

9.1 The Data Protection (Charges and Information) Regulations 2018 requires organisations that process personal information to pay a fee to the Information Commissioner's Office (ICO), unless exempt. The Information Commissioner maintains a public register of notified Data Controllers. The Council is registered under entry number Z5004355. Payment of the data protection fee on behalf of the Council is the responsibility of the Head of Legal, Democratic, Digital and Customer Services.

9.2 Individual Elected Members are exempt by law from payment of the data protection fee.

## 10.0 Documentation of Processing Activities

10.1 There is a legal requirement to document Processing activities under the Data Protection Legislation. The Council has an Information Asset Register (IAR) which forms the basis of the Council's documentation of Processing activities. It is the responsibility of each Service to update the IAR and ensure that the information relevant to their Service is accurate at all times.

## 11.0 Contracts

11.1 Where an organisation processes Personal Data on behalf of the Council there must be a contract in place that contains the Council's Terms and Conditions, which includes the Council's standard data protection clauses.

## 12.0 Data Sharing

12.1 Data sharing takes place when Personal Data is shared with another organisation for its own purposes. This is separate from when the organisation is Processing the Personal Data on behalf of the Council.

12.2 An appropriate written agreement for the sharing of Personal Data (known as a data sharing agreement or an Information Sharing Protocol) must be agreed and put in place for instances of one-off sharing as well as planned and regular sharing of Personal Data between the Council and other partners and before any systematic or large scale Personal Data sharing takes place. Legal, Democratic, Digital and Customer Services must be consulted prior to any such agreement being made. The Council's Information Sharing Protocol is available on ICON.

12.3 Completed Data Sharing Agreements should be sent to the Information Governance Team. A register of completed Data Sharing Agreements and Information Sharing Protocols is maintained by Legal, Democratic, Digital and Customer Services. These will be reviewed, amended and updated on a regular basis in accordance with operational requirements.

## 13.0 Data Protection Impact Assessments

13.1 A Data Protection Impact Assessment (DPIA) will be undertaken to identify and minimise the privacy risks of any new project or policy that will involve Processing Personal Data. The lead officer for the project or policy will be responsible for ensuring that the DPIA is undertaken. The DPO will assist Services to identify the need for a DPIA, provide guidance for the assessment process, and make recommendations to ensure the Council's compliance with the Data Protection Legislation.

13.2 Completed DPIAs should be sent to the Information Governance Team. A register of completed DPIAs is maintained by Legal, Democratic, Digital and Customer Services.

## 14.0 Data Breaches

14.1 The Council has a legal responsibility to ensure that Personal Data is processed securely, held confidentially and with integrity and accessed by only those who have a justified right of access. Despite the security measures taken to protect Personal Data held by the Council, a breach can happen.

14.2 The Council has a Data Breach Management Protocol which is to be followed in the event of a data breach.

14.3 It is a criminal offence under Data Protection Legislation to knowingly or recklessly obtain, disclose or procure Personal Data without the consent of the Data Controller and the Council reserves the right to report any such incidences to the Information Commissioner's Office and/or Police Scotland.

## 15.0 Governance

15.1 The Information Governance Steering Group (IGSG) will act as the forum for the consideration of any matters related to Data Protection Legislation and Policy. This Policy will be reviewed at least every 3 years.

15.2 Services will identify key contacts to comprise of the membership of the IGSG.

## 16.0 Conclusion

16.1 The Council subscribes to the principles of the Data Protection Legislation and will continue to develop policies, procedures and guidelines to ensure compliance with its legal obligations.

## Appendix 1

Data Protection Key Principles

a. Personal Data shall be processed fairly, lawfully and in a transparent manner.

b. Personal Data shall be processed only for the purposes for which it was obtained.

c. Personal Data shall be adequate, relevant and not excessive.

d. Personal Data shall be accurate and kept up to date where necessary.

e. Personal Data shall be kept in a form which permits identification of Data Subjects for no longer than is necessary for the purposes for which the Personal Data was processed.

f. Personal Data shall be processed in a manner that ensures appropriate security of the Personal Data.

As a Data Controller, the Council is responsible for, and must be able to demonstrate compliance with, these key principles.

## Appendix 2

**Inverclyde Council – policy statement and additional safeguards on Processing Special Category Data and Personal Data relating to criminal convictions and offences**

**Introduction**

With effect from 25 May 2018, Data Protection Legislation requires Controllers who process Special Category (i.e. sensitive) Personal Data, (or Personal Data relating to criminal convictions and offences) under various parts of the Data Protection Act 2018 to have an "appropriate policy document" in place setting out a number of additional safeguards for this data.

More specifically, the law states that:

> "The Controller has an appropriate policy document in place in relation to the Processing of Personal Data… if the Controller has produced a document which –
>
> explains the Controller's procedures for securing compliance with the principles in Article 5 of the UK GDPR (principles relating to Processing of Personal Data) in connection with the Processing of Personal Data in reliance on the condition in question, and
> explains the Controller's policies as regards the retention and erasure of Personal Data processed in reliance on the condition, giving an indication of how long such Personal Data is likely to be retained."

This document is the policy adopted by Inverclyde Council in relation to this Processing and fulfils the above test.

Policy Statement

1: Lawfulness, fairness and transparency:

All data which flows into and out of the Council has been assessed to determine the legal basis under which that data is processed and the results of the assessment have been documented in an Information Asset Register. The Council is satisfied that it has a legal basis for holding Personal Data, and that it also has a valid legal basis for disclosing this Personal Data to third parties where this takes place. Privacy notices have been prepared to comply with UK GDPR requirements (and to reflect the legal basis of Processing). Please see Privacy - Inverclyde Council for further details.

2: Purpose limitation:

The purposes for which data is collected are clearly set out in the relevant privacy notices. A limited set of data is required for research and archiving purposes; the Council has put in place appropriate safeguards for these activities as required by Article 89 of the UK GDPR.

3: Data minimisation:

In assessing the data flows, the Council has also taken the opportunity to assess the need for each of the data fields in question and will cease to capture unnecessary data.

4: Accuracy:

The Council checks data for accuracy and, where any inaccuracies are discovered, these are promptly corrected and any third party recipients of the inaccurate data notified of the correction.

5: Storage limitation:

The Council only keeps personal information for the minimum period necessary. Sometimes this time period is set out in the law, but in most cases it is based on business need. The Council maintains a Records Retention and Disposal Schedule which sets out how long the Council holds different types of information for. You can view this on the Council's website at Data Protection Policy - Inverclyde Council.

Ongoing management of the Council's records and information is subject to the provisions of the Council's Records Management Plan, which was developed in terms of the Public Records (Scotland) Act 2011 and approved by the Keeper of the Records of Scotland. This is available online at Records Management Plan - Inverclyde Council. The Records Management Plan sets out, in much greater detail, the provisions under which the Council complies with its obligations under public records legislation, data protection and information security and is complementary to this policy statement.

6: Integrity and confidentiality:

The Council has Security Guidelines which provides employees with guidance on how to keep personal, commercial and sensitive information secure and to share only in so far as is operationally necessary. In addition, the Council has an Acceptable Use of Information Systems Policy. All employees are required to complete information security training. The Council's ICT systems have appropriate protective measures in place incorporating defence, and the systems are subject to external assessment and validation. Policies and procedures are in place to reduce the information security risks arising from use of hard copy documentation.