Inverclyde council

AGENDA ITEM NO: 15

Report To:	**Policy and Resources Committee**	**Date:**	**19 November 2019**
Report By:	**Head of Legal & Property Services**	**Report No:**	**LP/136/19**
Contact Officer:	**Andrew Greer**	**Contact No:**	**01475 712498**
Subject:	**Data Protection Policy**		

1.0 PURPOSE

1.1 The purpose of this report is to provide the Policy & Resources Committee with an overview of the amended Data Protection Policy in the **Appendix**; and to seek the Committee's approval of this amended Policy.

2.0 SUMMARY

2.1 Data Protection Legislation has recently undergone significant changes with the introduction of the General Data Protection Regulation and the Data Protection Act 2018.

2.2 These changes have been incorporated into the Data Protection Policy which had previously been approved by the Committee on 5 February 2013.

2.3 The Policy sets out the Council's commitment to ensuring that any personal data, including special category personal data, which the Council processes, is carried out in compliance with the data protection legislation.

2.4 Given that this area of law is undergoing regular changes, the Policy will be reviewed in November 2020.

3.0 RECOMMENDATIONS

3.1 It is recommended that the Policy and Resources Committee approves the amended Data Protection Policy.

Gerard Malone
Head of Legal & Property Services

4.0 BACKGROUND

4.1 Data protection legislation changed significantly with the introduction of the Data Protection Act 2018 on 23 May 2018 and the General Data Protection Regulation on 25 May 2018. The data protection legislation sets out requirements on how organisations need to handle personal data and has enhanced the rights of individuals whose data is held and gives them more control over what happens to their data.

4.2 These changes have been incorporated into the Data Protection Policy, which had previously been approved by the Committee on 5 February 2013.

4.3 As well as ensuring compliance with the data protection legislation, the Policy will provide Services with updated guidance outlining the responsibilities of employees.

4.4 This report provides a summary of the main changes to the Council's Data Protection Policy.

5.0 NEW SECTIONS OF THE DATA PROTECTION POLICY

5.1 Definitions

5.2 A new definitions section has been created to assist employees with interpretation of key concepts of data protection. The key definitions remain largely the same as the previous legislation with the exception of Personal Data which has been expanded, and Special Category Data, previously known as Sensitive Personal Data.

5.3 Senior Information Risk Owner (SIRO)

5.4 Whilst not a new change brought about by the data protection legislation, the role of the Council's Senior Information Risk Owner (SIRO) has been included in the Policy to assist clarification. The SIRO has overall responsibility for Information Management and Information Risk Management within the Council.

5.5 Role of Data Protection Officer

5.6 The data protection legislation introduced a mandatory requirement for the Council to have a Data Protection Officer (DPO). The Policy provides a summary of the role of the DPO.

5.7 Special Category Data

5.8 As advised in paragraph 5.2, Special Category Data replaces the category of sensitive data and now consists of:

- Racial or ethnic origin.
- Political Opinions.
- Religious or philosophical beliefs.
- Trade Union membership.
- Genetics.
- Biometrics (where used for ID purposes).
- Health.
- Sex Life.
- Sexual Orientation.

5.9 Data Protection Fee

5.10 Previously the Council was required to register as a Data Controller with the Information Commissioner's Office (ICO) and pay a fee of £500. The Council no longer requires to register, however, the Council does require to pay a data protection fee of £2,900 on a corporate basis and the Head of Legal and Property Services will arrange payment of this fee on behalf of the Council.

5.11 Under the new legislation, Elected Members no longer require to register and are exempt by law from the data protection fee.

5.12 Documentation of Processing Activities

5.13 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.

5.14 Contracts

5.15 The data protection legislation introduced a mandatory requirement that the Council, when acting as Data Controller, must have a written contract in place with a Data Processor (the supplier), when processing personal data on behalf of the Council. For example:

- IT system purchased to store personal data;
- Shredding company hired to destroy personal data;
- An organisation contracted to carry out an administrative function on behalf of the Council.

5.16 This has been included in the Policy to ensure Services are aware of this important step.

5.17 Data Sharing

5.18 The Policy explains when there will be a need for a data sharing agreement, focusing on systematic or large scale data sharing, and directs Services to the Information Sharing Protocol available on ICON.

5.19 Data Protection Impact Assessments

5.20 The Policy explains when a Data Protection Impact Assessment may be required, focusing on minimising risks, and directs Services to the Data Protection Impact Assessment Guidance on ICON.

5.21 Appropriate Policy Document

5.22 The data protection legislation requires Data Controllers who process Special Category (or Personal Data relating to criminal convictions and offences) to have an "appropriate policy document" in place setting out a number of additional safeguards for this data. The Council's Appropriate Policy Statement is provided for in the Data Protection Policy Appendix 2.

5.23 **CHANGES TO EXISTING SECTIONS OF THE DATA PROTECTION POLICY**

5.24 Rights of Data Subjects

In addition to the extension of existing rights, the new data protection legislation introduces:

- Right of erasure in certain circumstances;
- Right to object to certain Processing; and
- Right to data portability.

These have been included in the Policy.

5.25 Data Breaches

5.26 The data protection legislation introduces far more strict timescales for reporting and completing any actions, and lowered the threshold for reporting data breaches to the ICO. The Policy makes reference to the Council's Data Breach Management Protocol to assist services manage data breaches effectively and timeously.

5.27 **OTHER CHANGES TO THE DATA PROTECTION POLICY**

5.28 All other changes are minor and include operational changes such as reference to the Information Governance Team; and additional changes introduced by the data protection legislation such as the Council demonstrating compliance with the data protection principles.

5.29 Given this area of law has recently undergone significant changes, the Data Protection Policy will be reviewed again in November 2020 to ensure that it continues to be relevant and accurate.

5.30 The Data Protection Policy will be the subject of briefings to members of the Extended Management Team during November/December 2019 and any practical items arising from implementation will be noted and reported upon for the November 2020 review, above.

5.31 In addition to the amended Data Protection Policy, the Information Governance Team has produced guidance on Subject Access Requests (SAR), which is the right of access by an individual to information held about them by the Council. The SAR Service Officers and the Information Governance Steering Group have been consulted and their feedback has been incorporated into the Guidance. SAR training will be delivered in May 2020 and the guidance on SARs will be readily available to all relevant officers.

6.0 IMPLICATIONS

6.1 Finance

Financial Implications:

One off Costs

Cost Centre	Budget Heading	Budget Years	Proposed Spend this Report	Virement From	Other Comments
N/A	N/A	N/A	N/A	N/A	N/A

Annually Recurring Costs/ (Savings)

Cost Centre	Budget Heading	With Effect from	Annual Net Impact	Virement From (If Applicable)	Other Comments
Council-wide Data Protection Fee	Data Protection Fee	25th May 2019	£2,900	N/A	New fee for Council Data Controller responsibilities.

6.2 Legal

The Council requires to take the steps as identified in this report to comply with data protection legislation.

6.3 Human Resources

There are no direct HR implications on this report.

6.4 Equalities

There is no direct effect upon equalities within this report.

(a) Has an Equality Impact Assessment been carried out?

☐ YES (see attached appendix)

X	NO – This report does not introduce a new policy, function or strategy or recommend a substantive change to an existing policy, function or strategy. Therefore, no Equality Impact Assessment is required

(b) Fairer Scotland Duty

If this report affects or proposes any major strategic decision:-

Has there been active consideration of how this report's recommendations reduce inequalities of outcome?

	YES – A written statement showing how this report's recommendations reduce inequalities of outcome caused by socio-economic disadvantage has been completed.
X	NO

(c) Data Protection

Has a Data Protection Impact Assessment been carried out?

	YES – This report involves data processing which may result in a high risk to the rights and freedoms of individuals.
X	NO

6.5 **Repopulation**

There is no implication for repopulation within Inverclyde.

7.0 CONSULTATIONS

7.1 The Information Governance Steering Group was consulted on the contents of the Policy and their input has been incorporated into the Policy.

7.2 The Corporate Management Team was briefed on the Policy on 23 October 2019 and endorses this report.

8.0 BACKGROUND PAPERS

8.1 Policy and Resources Committee Report – 2 February 2013 - https://www.inverclyde.gov.uk/meetings/meeting/1565

DATA PROTECTION POLICY

Version 02.2

Produced by:
Information Governance Team
Inverclyde Council
Municipal Buildings
GREENOCK
PA15 1LX

October 2019

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER
THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

.

Official

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
Information Governance Team	Data Protection Policy	Legal and Property 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

Distribution		
Name/ Title	**Date**	**Comments**
Legal Services	August 2019	Clarifying matters including role of Data Processors
Information Governance Steering Group	15th – 22nd October 2019	Minor amendments regarding structure.
Corporate Management Team	24th October 2019	Minor amendments.
Extended Management Team	November/December 2019	
Policy and Resource Committee	19th November 2019	

Distribution may be made to others on request

Policy Review			
Updating Frequency	**Review Date**	**Person Responsible**	**Service**
3 years unless required earlier	November 2020 (earlier review date to assess policy given new legislation)	Information Governance Team	Legal & Property Services

Document Review & Approvals: this document requires the following approvals:			
Name	**Action**	**Date**	**Communication**
Policy and Resources Committee		November 2019	

Linked Documentation *(Documents that you have linked or referenced to in the text of this document)*

Document Title	Document File Path

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.

Other key Council documents which are complementary to and which should be considered alongside this Policy include:

1. Acceptable Use of Information Systems Policy
2. Records Management Policy
3. Policy for Retention and Disposal of Records
4. Records Management Plan
5. Data Protection Breach Management Protocol
6. Data protection Impact Assessment Guidance
7. GDPR Employee Guide
8. Privacy Notices and Privacy Notice Guidance

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

- collected lawfully;
- used fairly;
- accurate and kept up to date;
- stored safely and securely;
- retained no longer than is necessary and;
- not disclosed to any third party unlawfully.

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 table below outlines key definitions that are referred to within this Policy and Data Protection Legislation

Personal Data	This is data which relates to a living individual ("Data Subject") who can be identified: • from the data. • from the data and other information which is in the possession of, or is likely to come into the possession of, the Data Controller. This includes the name, address, telephone number, national insurance number as well as any expression of opinion about the individual and any indication of the intentions of the Data Controller or any other person in respect of the individual.
Special Category Personal Data	This is Personal Data consisting of information as to any of the following: • Racial or ethnic origin. • Political opinions. • Religious or philosophical beliefs. • Trades Union membership. • Genetics. • Biometrics (where used for ID purposes). • Health. • Sex Life. • Sexual Orientation.
Record	A record is recorded information, in any form, including data in systems created, received and maintained by the Council and kept as evidence of such activity.
Subject Access Request	This is a right of access by individuals to their Personal Data held by the Council.
Records Management	The control of the Council records during their lifetime, from creation to storage until archiving or destruction.
Processing	The definition of Processing covers everything from obtaining and gathering in information to using the information and, eventually, destroying the information.
Data Controller	A Data Controller is a 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	This role is carried by any person other than a Council employee (for example, contractors and agents) who process personal information on behalf of the Council.
Data Protection Legislation	The General Data Protection Regulation EU 2017/679 (GDPR) and the Data Protection Act 2018.

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 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.

3.3 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.

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

4.8 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.

4.9 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 Corporate Director of the Inverclyde Health and Social Care Partnership (HSCP).

4.10 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:

Andrew Greer
Data Protection Officer
Inverclyde Council
Municipal Buildings
Greenock PA15 1LY
dataprotection@inverclyde.gov.uk
Tel: 01475 712498

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 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 Data Subject Rights

7.1 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.

7.2 The Council will ensure that the rights of Data Subjects are respected. Advice can be sought by contacting the Information Governance Team by email: dataprotection@inverclyde.gov.uk or by telephone: 01475 712498.

8.0 Data Protection Fee

8.1 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. Payment of the data protection fee on behalf of the Council is the responsibility of the Head of Legal & Property Services.

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

9.0 Documentation of Processing Activities

9.1 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.

10.0 Contracts

10.1 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.

11.0 Data Sharing

11.1 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.

11.2 An appropriate written agreement for the sharing of Personal Data (known as a data sharing agreement or an Information Sharing Protocol) must be in place before any systematic or large scale Personal Data sharing takes place. Legal and Property Services must be consulted prior to any such agreement being made. The Council's Information Sharing Protocol is available on ICON.

11.3 Completed Data Sharing Agreements should be sent to dataprotection@inverclyde.gov.uk. A register of completed Data Sharing Agreements and Information Sharing Protocols is maintained by Legal and Property Services.

12.0 Data Protection Impact Assessments

12.1 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.

12.2 Completed DPIAs should be sent to dataprotection@inverclyde.gov.uk. A register of completed DPIAs is maintained by Legal and Property Services.

13.0 Data Breaches

13.1 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.

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

13.3 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.

14.0 Governance

14.1 The Information Governance and 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.

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

15.0 Conclusion

15.1 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

(1) Personal data shall be processed fairly, lawfully and in a transparent manner.

(2) Personal data shall be processed only for the purposes for which it was obtained.

(3) Personal data shall be adequate, relevant and not excessive.

(4) Personal data shall be accurate and kept up to date where necessary.

(5) 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.

(6) 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 –

(a) explains the Controller's procedures for securing compliance with the principles in Article 5 of the GDPR (principles relating to Processing of Personal Data) in connection with the Processing of Personal Data in reliance on the condition in question, and
(b) 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 GDPR requirements (and to reflect the legal basis of Processing). Please see https://www.inverclyde.gov.uk/privacy for further details.

2: Purpose limitation:

The purposes for which data are 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 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 https://www.inverclyde.gov.uk/law-and-licensing/freedom-of-information.

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 https://www.inverclyde.gov.uk/council-and-government/strategies-policies-and-plans/records-management-plan. 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.