Inverclyde council

AGENDA ITEM NO: 19

Report To:	**Policy & Resources Committee**	**Date:**	**21 May 2019**
Report By:	**Head of Legal & Property Services**	**Report No:**	**LP/075/19**
Contact Officer:	**Andrew Greer**	**Contact No:**	**01475 712498**
Subject:	**Information Sharing Protocol**		

1.0 PURPOSE

1.1 The purpose of this report is to provide the Policy & Resources Committee with an overview of the amended Information Sharing Protocol in the **Appendix** and to seek the Committee's approval of this amended policy.

2.0 SUMMARY

2.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018 and introduced significant changes to the rules regarding data sharing.

2.2 The Information Sharing Protocol (ISP) was previously approved by the Policy and Resources Committee on 17 November 2015. It requires to be updated to reflect the new requirements of GDPR.

2.3 Given that this area of law is undergoing regular changes, the ISP will be reviewed again in May 2020.

3.0 RECOMMENDATIONS

3.1 It is recommended that the Policy and Resources Committee approves the Inverclyde Council Information Sharing Protocol.

Gerard Malone
Head of Legal & Property Services

4.0 BACKGROUND

4.1 The General Data Protection Regulation (GDPR) came into effect on 25 May 2018 and introduced new requirements for data sharing. These changes have been incorporated into the Information Sharing Protocol (ISP), which had previously been approved by the Committee on 17 November 2015.

4.2 The aim of the ISP is to help ensure that the Council fulfils its obligations under the GDPR when sharing data with relevant parties. The ISP will give services guidance and assistance to help identify where a Data Sharing Agreement (DSA) may be required. It will also provide a template for Services to complete an initial draft before sending to Legal and Property Services for review and approval.

4.3 The main changes to the ISP include 3 new template data sharing agreements listed in Appendices 1 – 3 of the ISP. The three template DSAs reflect the different relationships which the Council may enter into when sharing information. These relationships can be outlined as:

- Appendix 1: Data Sharing between Council Services (Internal);
- Appendix 2: Data Sharing between Council and one other Public body (External);
- Appendix 3: Data Sharing between Council and third party private organisation (External)

4.4 All other changes are minor and include operational changes such as reference to the Information Governance Team; and additional changes introduced by GDPR, such as privacy notices; updated legislation, and alternative options to consent for local authorities to use as a lawful basis.

4.5 These templates are a guide rather than being mandatory. It has been strongly recommended to services that the template wording is used unless there are clear reasons to depart from this standard. It has also been recommended to services that legal advice is sought on a case by case basis. As stated at paragraph 4.2, Legal and Property Services will require to review DSAs before they are signed off.

4.6 DSAs which predate this updated Information Sharing Protocol or the General Data Protection Regulation are being reviewed and will be registered in a corporate DSA register, administered by the Information Governance Team.

4.7 Training on the ISP and guidance will be delivered to key contacts within services by the Information Governance Team.

5.0 IMPLICATIONS

5.1 **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
N/A	N/A	N/A	N/A	N/A	N/A

5.2 **Legal**

The Council requires to take the steps as identified in this report to comply with the General Data Protection Regulation.

5.3 **Human Resources**

There are no direct HR implications on this report.

5.4 **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

5.5 **Repopulation**

There is no implication for repopulation within Inverclyde.

6.0 CONSULTATIONS

6.1 The GDPR Implementation Group were consulted on the contents of the ISP and their input has been incorporated into the ISP and associated guidance.

7.0 BACKGROUND PAPERS

7.1 Policy and Resources Committee Report – 17 November 2015 - https://www.inverclyde.gov.uk/meetings/meeting/1821

APPENDIX

Inverclyde council

Information Governance and Management Framework

Information Sharing Protocol

Version 2.1

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

2019

INVERCLYDE COUNCIL IS AN EQUAL OPPORTUNITIES EMPLOYER

THIS POLICY BOOKLET IS AVAILABLE ON REQUEST, IN LARGE PRINT, BRAILLE, ON AUDIOTAPE, OR COMPUTER DISC.

DOCUMENT CONTROL

Document Responsibility		
Name	**Title**	**Service**
Chief Officer, ICHCP	Information Sharing Protocol	Legal and Property Services

Change History		
Version	**Date**	**Comments**
0.1	March 2015	Draft for comments
0.1	October 2015	Amendments
1.0	17 November 2015	Approved
2.0	January 2019	Draft for comments
2.1	7 February 2019	Approved

Distribution		
Name/ Title	**Date**	**Comments**
GDPR Implementation Group	January 2019	Minor comments.

Distribution may be made to others on request

Policy Review		
Review Date	**Person Responsible**	**Service**
May 2020	Information Governance Team	Legal and Property Services

1 INTRODUCTION

1.1 This Protocol describes Inverclyde Council's policy and procedures in relation to the sharing of information and data within Council functions and among the Council and its partner organisations. It provides a framework within which information sharing can be encouraged and developed whilst being kept consistent with the Council's legal duties and responsibilities.

1.2 This Protocol applies to all data, hard copy and electronic, and information held by or used by the Council, which has been classed as "OFFICIAL" in terms of the Council's Classification Policy. For all practical purposes, the terms "data" and "information" as used in this Protocol are synonymous.

1.3 The Protocol includes the general principles to be applied to information sharing as well as providing three template Data Sharing Agreements (DSAs). The use of the template DSAs will vary depending on the purpose of the information sharing and this will be explored further in section 5.

1.4 The Protocol is not automatically or contractually binding on the Council's partners but is to be used to set good practice standards and expectations that the parties need to meet in order to comply with relevant legal duties and organisational policies which relate to the sharing of information. This does not prevent any Council service area from including the Protocol in any contractual or other formal agreement.

1.5 The Protocol is primarily concerned with the sharing of data, which is the provision of data by one party to another for the receiving party to use for its own purposes i.e. where all parties are data controllers. This protocol is not primarily concerned with data processing, where the receiving party uses data from a supplier or where the supplier acts as data processor and is not a data controller. Circumstances where one organisation receives data to be processed on behalf of another, is not information sharing and should be covered by a Data Processing Agreement, or advice should be sought from Legal and Property Services to ensure appropriate Data Protection Conditions are included as Special Conditions of Contract.

1.6 In circumstances where sharing involves commercially sensitive information, e.g. at the exploratory stage of a possible shared service project, the parties may wish to consider using a confidentiality agreement.

1.7 This Protocol should be read in conjunction with the Council's Information Classification Policy.

2 APPLICABILITY

2.1 Within the Council, all Council services are required to apply the principles of this Protocol to any information sharing activities, whether with external partners or other Council service areas. All Data Sharing Agreements are to be registered in the corporate repository by contacting the Information Governance Team at dataprotection@inverclyde.gov.uk.

2.2 The Council's partner organisations are requested to confirm their agreement to the principles contained in this Protocol in addition to any formal contracts or Data Sharing Agreements.

3 GENERAL PRINCIPLES

3.1 The general principles of this Information Sharing Protocol are as follows:

- there is a presumption in favour of sharing information, providing legislative and contractual requirements and restrictions or those of accepted good practice are followed;
- each identified data set or information asset will have a designated Information Asset Owner who is responsible for its proper security, integrity and use; and
- the specific requirements of any agreed exchange of data are to be recorded in a Data Sharing Agreement conform to the standard set out in this Protocol.

3.2 This Protocol is enforced and monitored through management arrangements which define the responsibilities of different service areas and individuals. The Council will manage this Protocol through the following governance framework structure:

- Information Governance Steering Group
- Records Management Working Group
- General Data Protection Regulation Implementation Group

4 LEGAL POLICY AND FRAMEWORK

4.1 All information sharing will be conducted within current and relevant legislation and guidance from the relevant public officials such as the Information Commissioner and the Scottish Information Commissioner.

4.2 Without any prejudice to the generality, for users' guidance the principal general laws or regulations concerning the protection and use of information affecting the Council and its functions are:

the Data Protection Act 2018
the General Data Protection Regulation 2016/679
the Freedom of Information (Scotland) Act 2002
Police and Fire Reform (Scotland) Act 2012the Rehabilitation of Offenders Act 1974
the Human Rights Act 1998 (in particular, Article 8)
the Criminal Procedure (Scotland) Act 1995Criminal Justice (Scotland) Act 2003the Regulation of Investigatory Powers (Scotland) Act 2000
the Housing (Scotland) Act 2001
the Local Government (Scotland) Act 2003
Protection of Vulnerable Groups (Scotland) Act 2007the Children (Scotland) Act 1995
the Children and Young People (Scotland) Act 2014
the Education (Scotland) Act 1980
the Education (Additional Support for Learning) (Scotland) Act 2004, as amended
the Equality Act 2010
the Adults with Incapacity (Scotland) Act 2000
the Antisocial Behaviour etc. (Scotland) Act 2004
the Social Security Administration Act 1992
the Carers (Recognition and Services) Act 1995
the Mental Health (Care and Treatment) (Scotland) Act 2003
the NHS and Community Care Act 1990
the Access to Medical Records Act 1990
the Management of Offenders (Scotland) Act 2005
the Health Service (Scotland) Act 1978 as amended by Health Service (Reform) (Scotland) Act 2004
the Public Records (Scotland) Act 2011
the Social Work (Scotland) Act 1968
the Copyright, Designs and Patents Act 1989
Common Law
Adult Support and Protection (Scotland) Act 2007
Children Hearings (Scotland) Act 2011
Public Bodies (Joint Working) (Scotland) Act 2014
Re-use of Public Sector Information Regulations 2015/1415; and

any other relevant or specific statute in relation to any Council function

4.3 The use of ICT systems to process and share data will also be subject to specific legislation governing the use of information technology, including the:

Computer Misuse Act 1990;
Electronic Communications Act 2000; and
Digital Economy Act 2010

4.4 The Council will also conform to the requirements of information security standards in general use including:
ISO 27002 – Code of Practice for Information Security Management

4.5 In addition, the Council operates its own policy framework for the management and security of information to extend and enforce these external standards. This framework and the policies and standards developed under it are available to Council staff on the internal repository of policies and standards and externally through links on the Council's web site. These policies include:

Data Protection Policy
Data Protection Breach Management Protocol
Records Management Policy
Policy for the Retention and Disposal of Documents and Records paper and Electronic.
Acceptable Use of Information Systems Policy
Information Classification Policy
Clear Desk Environment
Guidance on Flexible, Mobile & Home Working
Homeworking Policy

4.6 These policies are currently being updated to reflect the General Data Protection Regulation and the Data Protection Act 2018. Further, updates will be provided on ICON.

4.7 The development of specific agreements or policies which enable or manage the efficient sharing of information is encouraged, provided they are consistent with the general principles contained in this Protocol.

5 DATA SHARING AGREEMENTS

5.1 Data Sharing Agreements (DSAs) are the key method of managing the sharing of information among partner organisations. DSAs must be agreed between Inverclyde Council service areas which are designated Information Asset Owners of information and any internal or external partners with whom information is to be shared.

5.2 DSAs must be consistent with the general principles of this Protocol but they can differ in detail where the specific activities of the Council service area and its partners require. The DSAs must however document all the requirements of the information sharing which is to take place.

5.3 DSAs (of whatever form) which predate this updated Information Sharing Protocol or the General Data Protection Regulation will require to be reviewed and must be registered in the corporate repository by contacting the Information Governance Team.

5.4 Three template DSAs are attached in Appendices 1 - 3, together with guidance notes on the various sections of the agreement form. The three template DSAs reflect the different relationships which the Council may enter into when sharing information. These relationships can be outlined as:

- Appendix 1: Data Sharing between Council Services (Internal);
- Appendix 2: Data Sharing between Council and one other Public body (External);
- Appendix 3: Data Sharing between Council and third party private organisation (External)

These templates are a guide rather than being mandatory. It is strongly recommended the templates are used unless there are clear reasons to depart from this standard. Legal advice should also be sought on a case by case basis.

Copies of Appendices 1-3 are available on request from Andrew Greer, Information Governance Officer (tel: 712498/email: andrew.greer@inverclyde.gov.uk)

5.5 Any request to share information that is not covered within an existing DSA should be directed to the appropriate Information Asset Owner on a 'data sharing request form' (Appendix 4). A decision will be made by the appropriate Information Asset Owner whether sharing can take place (Appendix 5)

5.6 In general, DSAs should refer to existing policies and standards but where these need to be extended or enhanced, the development of new policies should follow the guidelines given in the section on Legal and Policy Framework above. These specific policies and standards should be consistent with the existing corporate standards. Any areas of potential disagreement or conflict are to be raised with the owner of the corporate policy or standard.

6 DATA PROCESSING AGREEMENTS

6.1 Information sharing refers to those situations in which the Council provides or receives data from another party which the receiving party uses for its own purposes. Where you receive personal data from another party, you should notify Legal & Property Services to ensure this is covered by the Council's existing Registration with the Information Commissioner.

6.2 Where data is supplied purely to be processed on behalf of the supplying organisation (such as part of an outsourcing agreement), a DSA is not required. These data transfers should be covered either by the Terms and Conditions of the Contract or by a separate Data Processing Agreement (DPA).

6.3 A specific DPA may need to be drawn up for each individual instance and it may be linked to or form part of a formal contract.

7 CORPORATE REPOSITORY OF DATA SHARING AGREEMENTS

7.1 The creation and maintenance of a comprehensive repository of DSAs is the key management component of this Protocol. The repository of DSAs allows the Council to understand what information sharing activities are currently being undertaken. It also helps minimise duplication and provides a method of ensuring the consistency of approach across all Council services.

7.2 The repository forms part of the policies, procedures and guidance database, which is managed by the Information Governance Steering Group. All DSAs are to be registered by submitting them for publication on the repository by contacting the Information Governance Team. The title of all DSAs will be made available openly to all Council Officers on the repository on ICON and the Information Governance Team will retain the substantive DSA. If Services wish to receive a copy of the substantive DSA and/or wish to share the substantive DSA with any third party organisation, they should contact the Information Governance Team.

8 SECURITY OF SHARED DATA

8.1 An appropriate level of information management and security requires to be assigned to the information exchanges envisaged by this Protocol. Parties must have appropriate policies in place covering the security, storage, retention and destruction of personal information in accordance with authoritative guidance issued to their organisations. The Council's most relevant policies are:

- Records Management Policy
- Policy for the Retention and Disposal of Documents and Records Paper and Electronic.
- Acceptable Use of Information Systems Policy.
- Data Protection Policy
- Information Classification Policy

8.2 The Council's policies and the policies of the organisation providing the information (depending on the agreement) must be applied to information shared under this Protocol being policies which are designed to protect the information (particularly, but not exclusively personal information) which they hold. The Council's policies are binding on all staff of the Council and misconduct or disciplinary action may be taken against any staff in contravention. These policies will apply to information held by that party, whether it has originated with that party or been passed to it by another party.

8.3 The parties will each ensure that the other parties are promptly notified and, in any event, no later than 24 hours after becoming aware of a breach or suspected breach, or significant security risks, affecting shared information. In addition, should the breach be considered significant, the ICO will also be notified. Instructions and guidance can be found in the Council's Data Protection Breach Management Protocol. The Parties will, where appropriate, work together to rectify any such breach or mitigate any such risk to information security. If personal data is lost as a result of a security breach, the parties will consider on a case by case basis whether to notify the affected individuals of the breach and other remedial and restitutive actions.

9 TRANSFERRING DATA

9.1 The most straightforward method of transferring data should be chosen but always with proper regard to any requirements of data security. In particular, personal data should never be transferred in an open format which is capable of being read easily if the data were lost, stolen or intercepted.

9.2 The Council provides methods of securing data, which generally involve encrypting it. Staff should contact ICT for guidance on transferring data securely and for requesting an encrypted USB memory device.

9.3 Consideration must always be given to the ability of the receiving partner organisation to operate the proposed secure method of transferring data.

9.4 Individual external partners may have data security requirements of their own, which the Council will consider meeting wherever practicable. These include the use of specific technical standards for encrypting data or the use of secure services for transmitting data. Any potential conflicts or areas of non-compliance with the Council's information security policies must be notified to the Information Governance Steering Group.

9.5 These transmission methods will generally be supported by the Council's technology partners. Responsibility for ensuring consistency with the Council's information security policies rests with the Information Governance Steering Group, which can also provide advice and guidance on security procedures.

9.6 Protective Marking: Information which is shared will carry a protective marking. The markings are as follows:

- No Classification
- Official
- Official - Sensitive

9.7 Parties undertake to take reasonable steps to ensure all data is properly protectively marked and used only in manner which is consistent with the agreed purpose under the DSA.

9.8 Access to data will be restricted to relevant and authorised persons, and where appropriate, to those who have signed a confidentiality agreement (or equivalent), and have received training in the General Data Protection Regulation and the Data Protection Act 2018. Data should only be processed in secure offices and shall not routinely be used or otherwise accessed out with the premises of parties.

9.9 Where it is considered necessary for personal information to be removed from office premises for meetings or approved home working, it should be carried securely, preferably on encrypted portable

media or a secure lockable case/box. Staff should refer to Home Working Policy/Guidance on Flexible, Mobile & Home Working. The information should remain in the possession of the individual at all times unless it can be stored in an approved security container. Special category and sensitive personal information should not be worked on anywhere where the contents might be seen, overlooked or otherwise noticed, and they should not be left unattended in any public place, such as a hotel, taxi or public transport vehicle. Relevant staff should have completed information security training in mobile working and out and about working.

10 MANAGEMENT AND MONITORING ARRANGEMENTS

10.1 Any formal framework or general agreement with partners should include a clear reference to the applicability of this Protocol to information sharing activities.

10.2 The management and monitoring of this Protocol include:

- responsibility for this Protocol and its application being with the Information Governance Steering Group;
- all Data Sharing Agreements will be lodged in the corporate repository;
- the Information Governance Team will manage this repository;
- the Information Governance Steering Group will initially provide a forum within the Council to oversee the management of the Protocol; and

questions or complaints about the operation of the Protocol, whether from within the Council or from external partners, should be referred in the first instance to the Information Governance Steering Group, which will ensure that they are dealt with by the appropriate Council service area.

11 DATA PROTECTION LAWS

11.1 All parties must adhere to the terms of the General Data Protection Regulation and the Data Protection Act 2018 insofar as any information being shared constitutes personal or special category/sensitive data. The management of personal data and its availability for sharing both within the Council and with external partners are governed by the Council's Data Protection Policy, which applies the relevant statutory provisions to the Council's own internal processes.

11.2 Any sharing of personal data must be both fair and lawful. Conditions for processing set out in the Data

Protection Laws must also be met, for example, the processing of the personal data is necessary for the Council to perform a public task or comply with the law or because of concerns or perceived risks regarding the welfare of the individual or others. This is evidenced in the Council's Corporate Privacy Notice which is available at https://www.inverclyde.gov.uk/privacy. Council Services will also have their own Privacy Notices which can be found at the same link under the heading "Privacy Notice Library All Council Services".

11.3 Legal advice should be sought if there is any doubt that the proposed sharing is lawful.

12 FREEDOM OF INFORMATION

12.1 The Council must respond to any proper request for recorded information made to them for the purposes of the Freedom of Information (Scotland) Act 2002 (FOISA). This includes obligations to respond to requests about information sharing practices and procedures in terms of this Protocol.

12.2 It should be noted, however, that the OFFICIAL information exchanged between parties may be exempt from disclosure under the FOISA. All parties should include reference to this Protocol in their respective publicly available Publication Schemes.

12.3 Any requests for information or data under the FOISA should be referred to the Freedom of Information/Data Protection Officer for each respective Party.

13 RECORDS GOVERNANCE

13.1 The Council's partner organisations involved in the sharing of data are expected to have a commitment to proper procedures and practices for:

- the retention and deletion of shared data items and procedures for dealing with cases where different organisations may have different statutory or professional retention or deletion rules;
- dealing with termination of any data sharing initiative, including the deletion of shared data or its return to the organisation that supplied it orginally; and,
- the sharing of datasets; to prevent irrelevant or excessive information being disclosed and to make sure the data being shared is accurate.

14 REVIEW AND MONITORING OF THIS INFORMATION SHARING PROTOCOL

14.1 This document will be reviewed every 2 years or more frequently if required.

15 ENFORCEMENT

15.1 The Council's Code of Conduct specifies it employees' obligations towards confidentiality. Every employee is required to respect the confidentiality of information about individuals or organisations. Any breaches of this principle will be viewed as a serious matter for the Council and its partners.

15.2 The Council's partners will be expected to take similar and proportionate actions in relation to any breaches of this Protocol and to investigate and act appropriately for the security of all information comprised within this Protocol.

Flowchart of Key Questions for Information Sharing