Highland Council
Data Protection Policy

Contents

Contents

1. Document Control

Version History

Version	Date	Author	Change
1	24/09/2013	Miles Watters	FHR Committee Approval
			Approved at FHR 09/10/2013
1.1	20/11/2013	Miles Watters	Amendment to 5.8 to add other areas recognised by EC. In recognition of Schedule 1, Part II Section 15 of the Act.
1.2	28/01/2015	Miles Watters	Annual review. Approved at Resource Committee 25/02/2015
1.3	07/04/2016	Miles Watters	Amendment of Sections 7 and 8 to reflect Internal Audit findings
2.0	17/04/2018	Miles Watters	Rewritten to reflect the requirements of the EU General Data Protection Regulation and the UK Data Protection Act 2018
2.1	31/05/2022	Miles Watters	Updated to reflect Brexit changes to data protection legislation. Approved at Corporate Resources Committee 01/12/2022

Document Authors

Miles Watters: Performance and Information Governance Manager

Distribution

Name	Role	Reason
	Corporate Resources Committee	Approval
	Information Governance Board	Review and acceptance
Kate Lackie	Executive Chief Officer, Performance & Governance and Senior Information Risk Owner	Review and acceptance

2. Introduction

The Highland Council is fully committed to compliance with the requirements of the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018 (DPA). The Council will take appropriate measures to ensure that all employees, elected members, contractors, agents, consultants and partners of the council who have access to any personal data, held by or on behalf of the Council, are fully aware of and abide by their duties and responsibilities under Data Protection Legislation.

3. Statement of policy and Scope

In order to operate efficiently, The Highland Council has to collect and use information about people with whom it works. These may include members of the public, current, past and prospective employees, clients and customers, and suppliers. This personal information must be handled and dealt with properly, however it is collected, recorded and used, and whether it is in paper or electronic format, and there are safeguards within the Data Protection Legislation to ensure this.

The Highland Council regards the lawful and correct treatment of personal information as very important to its successful operations and to maintaining confidence between the Council and those with whom it carries out business. The Council will ensure that it treats personal information lawfully and correctly.

To this end the Council fully endorses and adheres to the Principles of Data Protection and to the principle of “Data Protection by design and default”.

This policy applies to all Highland Council employees, agents of the Council, persons representing the Council (including sub-contractors and consultants), Trade Union representatives and Elected Members.

4. Glossary of terms

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;

Special Categories of personal data
Special categories of personal data means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

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.

Conditions for processing
The legislation provides conditions for the processing of any personal data. It also provides separate conditions for processing "personal data" and "special categories of personal data".

Some processing of personal data carried out by certain parts of the Council, which carry out enforcement activities, are not subject to the UK GDPR. This processing comes under the definition of "law enforcement processing" is subject to Part 3 of the DPA. This affects Criminal Justice, Trading Standards, Environmental Health and Planning Enforcement.

Appendix 1 gives the conditions for processing as contained in Articles 6 and 9 of the UK GDPR and Section 31 of the DPA (Law enforcement purposes).

5. Handling of personal data

The legislation stipulates that anyone processing personal data must comply with six principles. These principles are legally enforceable.

The Highland Council will, through appropriate management and controls, adhere to the principles of data protection. The principles are listed below.

5.1 Principle 1 – Lawfulness, fairness and transparency

Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject; [UK GDPR Article 5(1)(a); Section 35 of the DPA]

Staff must be aware of the reasons for which they process personal data and be able to explain this to the data subject. The Council has prepared privacy notices which will assist with this explanation and which state the conditions under which personal data is processed for a specific purpose.

Personal data may not be processed unless one of the conditions of Article 6, Article 9 or the Law Enforcement purpose applies (see appendix 1).

5.2 Principle 2 – Purpose limitation

Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes; [UK GDPR Article 5(1)(b); Section 36 of the DPA]

Data subjects must be informed of all purposes for which their data will be used at the time of collection. Services must ensure that privacy notices contain clear explanations of how data will be used. Any use of personal data for statistical analysis shall be governed by

these 6 principles.

5.3 Principle 3 – Data minimisation

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed; [UK GDPR Article 5(1)(c); Section 37 of the DPA]

This means that the Council shall only collect the specific data necessary to complete a given task. It would be a breach of principle 3 to collect additional data.

5.4 Principle 4 – Accuracy

Personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay; [UK GDPR Article 5(1)(d); Section 38 of the DPA]

This depends on the nature of the data being processed. In some cases data will not change over time, whereas in other cases data will be updated on a regular basis. In all cases the Council must ensure the accuracy of the data being processed.

5.5 Principle 5 – Storage limitation

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 are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) subject to implementation of the appropriate technical and organisational measures required by this Regulation in order to safeguard the rights and freedoms of the data subject; [UK GDPR Article 5(1)(e); Section 39 of the DPA]

All managers and staff will adhere to the Council's Records Management Policy and ensure that the Council's Corporate Retention Schedules are adhered to.

5.6 Principle 6 – Integrity and confidentiality

Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures; [UK GDPR Article 5(1)(f); Section 40 of the DPA]

All managers and staff within the Council's Services will comply with the Council's information security and information management policies. They will take steps to ensure that personal data is kept secure at all times against unauthorised or unlawful loss or disclosure, and in particular will ensure that:

- Paper files and other records or documents containing personal/sensitive data are kept in a secure environment;
- Personal data held on computers and computer systems is protected by the use of

secure passwords, which comply with the Council's password policy

- Personal data held on portable devices is encrypted.

5.7 Additional measures

In addition to adhering to the principles of Data Protection, The Highland Council will ensure that:

- A Data Protection Officer is appointed in compliance with Articles 37 to 39 of UK GDPR and Sections 69 to 71 of the DPA;
- Everyone managing and handling personal data understands that they are contractually responsible for following good data protection practice;
- Everyone managing and handling personal information is appropriately trained to do so;
- Everyone managing and handling personal information is appropriately supervised;
- Anyone wanting to make enquiries about handling personal information, whether a member of staff or a member of the public, knows what to do;
- Queries about handling personal information are promptly and courteously dealt with;
- Methods of handling personal information are regularly assessed and evaluated;
- All projects and changes which affect the use of personal data will follow the principle of Data Protection by design and default;
- Regular and systematic data sharing is carried out under a written agreement as described below.

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

6. Data Subject Rights

Data Subjects have a number of rights under Data Protection Legislation:

- The right to be informed (UK GDPR Articles 13 & 14; DPA Section 44) (see section 7)
- The right of access (UK GDPR Article 15; DPA Section 45)
- The right to rectification (UK GDPR Article 16; DPA Section 46)
- The right to erasure (UK GDPR Article 17; DPA Section 47 & 48)
- The right to restrict processing (UK GDPR Article 18; DPA Section 47 & 48)
- The right to data portability (UK GDPR Article 20)
- The right to object (UK GDPR Article 21)
- Rights in relation to automated decision making and profiling (UK GDPR Article 22; DPA Section 49)

Each of these rights has a common set of standards which the Council must adhere to:

- Requests must be in writing but the Council must accept requests submitted by

email or other electronic means.

- The Council may request identification to ensure that the information is provided to the right person.
- All requests must be responded to in one month (30 calendar days).
- Where the Council fails to respond in one month it must provide an explanation and inform the data subject of their right to contact the Information Commissioner's Office to complain.
- The response time can be extended by two months if the request is complex. The Council must inform the data subject of the extension within the first month and provide an explanation.
- Information must be provided free of charge unless the request has already been answered.
- The information provided in a response must be clear, concise and in plain English.
- The Council does not have to respond to requests that are considered "manifestly unfounded or excessive" and the Council can charge a reasonable fee to cover the costs of complying with these requests. In these cases the Council must provide an explanation which demonstrates that the request is unreasonable.

A full explanation of these rights and when they can and can't be accessed is given on the Council's website – www.highland.gov.uk/data-protection

A form is available on the Council's website to enable Data Subjects to submit requests and guidance for staff on how to deal with requests is available on the Council's intranet. Separate guidance on how to deal with access requests is also available to staff on the intranet.

All Data Subject requests will be recorded on the Council's Customer Relationship Management System to enable requests to be managed and to enable performance reporting.

7. The right to be informed

Unlike the other data subject rights, where the data subject must make a request in writing to the Council, the right to be informed is an obligation (under Articles 13 & 14 of UK GDPR and section 44 of the DPA) for the Council to provide information to data subjects at the time that personal data is first collected for a specific purpose.

This obligation is met through the provision of privacy notices specific to the purposes for which the Council processes personal data. A privacy notice must provide the following information:

- The identity and contact details of the Council (Data controller).
- Contact details for the Council's Data Protection Officer.
- A clear description of the purposes of the processing and the legal basis for carrying out the processing including which condition under Article 6(1) of UK GDPR applies.
- If the data is required for statutory reasons or in relation to a contract, the consequences of failing to provide the data must be provided.
- Whether the data will be shared and details of who the data will be shared with.
- Whether the data will be transferred to a 3rd Country (see section 8).

- The period for which the data will be stored.
- Details of the data subject rights which apply.
- If consent is the basis for processing, you must explain how to withdraw consent.
- Details of the right to complain to the ICO and contact details.
- Where data is processed automatically or used to create a profile of the data subject, details of this processing must be provided.

The Council's privacy notices are published on the Council's website.

8. Transfer to third Countries

Both the UK GDPR and the DPA put restrictions on the transfer of personal data to countries out with the UK ("third countries"). These restrictions are intended to ensure that the level of protection for personal data is not undermined by such transfers.

Transfers may take place to third countries which are the subject of "adequacy regulations" by the UK Government. Currently these countries and territories are Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, Iceland, Norway, Liechtenstein, Gibraltar, Andorra, Argentina, Faroe Islands, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Switzerland, Uruguay, Japan (only private sector organisations), and Canada (only covers data subject to Canada's Personal Information Protection and Electronic Documents Act).

Transfers may also take place where the recipient in the third country has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available. Examples of appropriate safeguards are

- Standard clauses adopted by the UK Government
- Binding corporate rules
- Contract clauses authorised by the Information Commissioner

The issue of transfer to third countries has the greatest impact on the Council in relation to ICT contracts especially those involving cloud based services. Information Asset Owners must ensure either that the data warehouses or server farms (including mirrored sites and backup sites) which are used to store their data are located within the UK or a third country which is subject to an adequacy agreement.

If this is not the case then appropriate safeguards, as outlined above, must be put in place prior to the transfer of personal data. The advice of the Data Protection Officer should be sought in relation to such issues.

In particular circumstances, and only on a case by case basis, it is possible to use derogations or exemptions to transfer personal data to a third country. However, no such transfers should be made without first seeking the advice of the Data Protection Officer.

9. Data processing agreements

The Council may use third parties or contractors to carry out the processing of personal data on its behalf. This processing may only take place under the written instruction of the Council and must comply with Article 28 of the UK GDPR (Section 59 of the DPA).

Data processing agreements must meet the following criteria:

- The agreement must be in writing.
- The processor must be able to provide sufficient guarantees that they are able to implement appropriate technical and organisational measures to ensure the protection of the personal data being processed on the Council's behalf.
- The processor may not appoint any sub processor without authorisation from the Council and the Council must be informed of any intended changes in relation to sub processors.
- The processor must remain liable for any sub processor(s) and the sub processor must be subject to the same obligations as the processor
- The processor must only process personal data under documented instruction from the Council.
- The processor must not make any decisions about the purposes for which the personal data may be processed.
- The processor's staff which process personal data must be subject to an obligation of confidentiality.
- The processor must ensure the security of processing.
- The processor must assist the Council in relation to Data Subject rights requests.
- The processor must assist the Council in relation to security, breach notification and data protection impact assessments.
- The processor must provide assistance with demonstrating compliance with data protection legislation and must cooperate with audits and inspection by the Council or their appointed auditor.
- The agreement must describe how personal data will be transferred back to the Council at the end of the agreement and securely deleted by the processor, unless there are legal reasons for the processor retaining the data

The above terms may be included in the main contract or can be the subject of a separate data processing agreement.

10. Joint Controllers

In some circumstances, the Council and a partner organisation or contractor may consider that both parties are involved in making decisions about the processing of personal data. Where two or more controllers jointly determine the purposes and means of processing, they are known as joint controllers.

In such circumstances, the roles and responsibilities of all parties must be clearly documented and made available to data subjects, to give data subjects an understanding

of how their personal data will be processed and by whom. It must be clear who the data subject should contact in each organisation to exercise their rights under the data protection legislation.

It must also be clear which party will fulfil the legislative requirements in relation to the provision of privacy notices to data subjects and these privacy notices should explain the joint controller relationship in a clear and transparent way.

11. Data Sharing

Data Protection legislation does not prohibit the sharing of personal data where it is appropriate. It may be appropriate to share personal data for a number of reasons including:

- There may be a legal requirement to share
- You may have received the consent of the data subject
- Sharing may be in the best interests of the data subject
- Sharing may be necessary to prevent or detect crime

It is the responsibility of Information Asset Owners to assess the nature of the relationship between the Council and other organisations (contractors, consultants, partners etc.) in terms of the control of personal data. This will enable them to decide whether they are joint controllers or whether a data sharing agreement or a data processing contract (see Section 9) is required in each specific case where personal data under the control of the Council is shared.

Where information is being shared either with a different organisation or internally, for a purpose other than that for which the data was collected, a data sharing agreement must be agreed. A data sharing agreement describes which condition for processing applies, the reason for sharing, the data to be shared and the key contacts in the organisations that the data is being shared with. It will also specify the purposes for which the shared information can be used.

Guidance on data sharing is available on the Council's intranet and the Information Commissioner's Office has produced a Code of Practice for Data Sharing.

The Highland Council has existing data sharing agreements in place with its key partner organisations such as NHS Highland, Police Scotland, The Scottish Fire and Rescue Service, Highlife Highland and the Scottish Government among others. Council staff must be familiar with any existing data sharing agreements which relate to their functions.

The Council will create and maintain a register of Data Sharing Agreements.

12. Data Protection Impact Assessments

Article 25 of the UK GDPR and Section 57 of the DPA place obligations on the Council to ensure that the protection of the rights and freedoms of data subjects is central to all processing of personal data. This is known as Data Protection by design and default. It requires the Council to ensure that all of its processing of personal data complies with each of the Data Protection Principles.

Data Protection Impact Assessments (DPIAs) are a useful tool to assist the Council with achieving this aim. The Information Commissioner has produced a handbook for DPIAs

and guidance on carrying out these assessments is available on the Council's intranet. The Data Protection Officer will provide advice and guidance in relation to DPIAs.

The Council will carry out DPIAs in the following circumstances:

- New projects or initiatives
- Data protection Audits
- Where a mandatory DPIA is required by the legislation

12.1 DPIA for new projects

The Information Commissioner's Office advocates that the protection of privacy through good data protection practice should be built into processes right at the start rather than being considered towards the end of a project and then requiring expensive changes. This complies with the obligation for Data Protection by design and default.

A DPIA will be carried out prior to implementing new procedures or systems or making changes to existing procedures or systems. By considering privacy at the very start of a new initiative, the system or process can be designed to have least privacy impact and also be more efficient.

The Council will carry out a privacy impact assessment for any new projects or systems which use personal data or have the potential to affect privacy. Project Boards must ensure that the requirement for a DPIA is agreed at project initiation.

An important aspect of a DPIA for new systems is to understand where the personal data is being stored, especially in relation to cloud storage, and to ensure that this complies with the rules around international transfers described in Section 8 above.

12.2 DPIA in Data Protection audits

One of the statutory tasks of the Data Protection Officer is to monitor compliance with the Data Protection Legislation. This will be carried out through the use of DPIAs to assess whether current practices comply with the Data Protection principles.

12.3 Mandatory DPIAs

Article 35 of the UK GDPR and Section 64 of the DPA require the Council to carry out a mandatory DPIA where the type of processing envisaged is likely to result in a high risk to privacy. Nine types of processing have been identified which are likely to result in a high privacy risk and the ICO will also publish a list of processing operations which require a mandatory DPIA. The nine types of processing are:

- Evaluation or scoring
- Automated decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combing data sets
- Data concerning vulnerable data subjects

- Innovative use or applying new technology or organisational solutions
- When the processing, in itself, prevents data subjects from exercising a right or a contract

If an Information Asset Owner is considering carrying out processing which fits within one of these nine criteria they must first contact the Data Protection Officer for advice.

It is envisaged that in the majority of cases DPIAs will be published.

13. Breaches

Where a breach of data protection occurs, it is important that the Council takes immediate steps to reduce the impact on those whose data is affected. The Council must also report breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach, where the breach will result in harm to the rights and freedoms on data subjects.

All Security breaches must be reported to the ICT Service Desk immediately. Where security breaches involve personal data, the Data Protection Officer must also be informed immediately. The Data Protection Officer may request that a data protection breach report is compiled. The breach report must provide details of the incident, how it occurred, steps taken to reduce the impact, steps taken to ensure that the same breach does not occur again and any lessons which should be shared within the Council to avoid similar incidents in other sections. The breach report must also include details about the numbers of people affected and the type of information involved.

Once completed, the breach report will be copied to the relevant Executive Chief Officer, as well as the Data Protection Officer. The Data Protection Officer is responsible for reporting the breach to the ICO and will usually provide a copy of the breach report.

If it is not possible to gather all the required information regarding a breach within the required 72 hours, the Data Protection Officer will contact the ICO to provide notification of the breach and inform them that further information is being gathered.

Staff with concerns around potential breaches of Data Protection should contact the Data Protection Officer for advice. Guidance on the breach procedure is available on the intranet.

14. Data Protection Fees

The Council is required by the Data Protection (Charges and Information) Regulations 2018 to pay an annual fee to the Information Commissioner's Office. The ICO has powers to serve monetary penalties on data controllers who refuse to pay the fee.

As well as the Council, the Highland Licensing Board is required to pay an annual fee. While all Councillors are considered to be data controllers in their own right, they are exempt from paying fees. The Data Protection Officer manages the payment of these fees.

15. Supporting Policies

This policy is complementary to and should be read in conjunction with the following

Information and Data Strategy
Information Management Policy
Records Management Policy
Records Retention & Disposal Policy
Information Security & Assurance Policy
ICT Acceptable Use Policy

16. Roles and responsibilities

This section sets out the general and specific responsibilities for ensuring that the principles of Data Protection are adhered to.

16.1 All Staff, and any person working on behalf of the Council

Data Protection is everybody's responsibility and is something that should be considered as a part of normal everyday working practice.

Staff and those handling Council information should understand the information that they create, receive and use and be able to identify information that is or may become a record and understand the security and data protection requirements. Information and records management processes that are in place must be followed and record keeping systems should be used in accordance with provided instructions and guidance.

All staff and those handling Council information must have completed the Information Management online learning module and any other relevant training that is required to use the records management systems and supporting ICT systems required in their role.

16.2 Managers and Supervisors

Managers are responsible for information held within their area. This includes ensuring that an up to date and maintained list of Information Assets is held and that this is entered into the Corporate Information Asset Register.

Managers and supervisors must ensure that all their staff have understood their obligations under this Policy (both general obligations and those that are specific to their role) and other Information Management Policies. Managers should support their staff in this regard by highlighting relevant parts of policies that apply to the roles being performed by a member of staff.

Managers and supervisors must ensure that all their staff have completed the Information Management online learning module and other relevant training. They should also ensure that staff are aware of any relevant data sharing agreements.

16.3 Information Asset Owners & System Owners

An Information Asset Owner is a person who has been identified as being responsible for a Highland Council Information Asset. A System Owner is a person who has been identified as being responsible for a Highland Council ICT System.

Information Asset Owners and System Owners must ensure that the management of their Information Asset is consistent with the principles of data protection and that the Council's Information Security & Assurance Policy is adhered to.

Information Asset Owners and System Owners must ensure that the information recorded in relation to their Information Asset in the Information Asset Register is correct and up-to-date.

16.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior person responsible for management of information security risks and for reporting this to the Executive Leadership Team. They are the corporate owner of the Information Governance strategies and policies The SIRO role is performed by the Executive Chief Officer, Performance and Governance.

16.5 Security Management

Information Security Incident Management and Investigations are managed by ICT Services on behalf of the Head of ICT and Digital Transformation.

16.6 Performance and Information Governance Manager

The Performance and Information Governance Manager is responsible for ensuring all Highland Council records are held within appropriate records management systems and structures. They are supported in this by the Records Manager and Records Management Service.

The Records Manager provides a Records Management Service to the Council under a Service Delivery agreement between the Council and Highlife Highland. This includes the provision of advice on records management, the management of the Council's Corporate Records Stores (including both paper records stores and the corporate electronic records store), and maintaining both the Council's Corporate Retention Schedules and Corporate Information Asset Register.

The Performance and Information Governance Manager, in conjunction with the Head of ICT and Digital Transformation, is also responsible for ensuring the Council's Information Security Management System, Information Management and Security Policies, and Information Security Incident Reporting processes support the Council's compliance with the Data Protection legislation.

16.7 Data Protection Officer

The Data Protection Officer is a statutory role which is set out in Articles 37 to 39 of the UK GDPR and Sections 69 to 71 of the DPA. Their tasks include:

- the provision of information and advice to Council managers and other staff in relation to the Data Protection legislation.
- monitoring the Council's compliance with data protection legislation and its own policies in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and related audits.
- the provision of advice in relation to data protection impact assessment and monitor the Council's compliance with the obligation to carry out mandatory DPIAs.
- acting as the contact point for the Information Commissioner's Office with regard to any matters relating to data protection.

- managing the process for dealing with requests all data subject rights requests
- providing advice and assistance to members of the public in relation to data protection

16.8 Responsible Premises Officer (RPO)

An RPO is responsible for the physical security of buildings through the effective management of perimeter security and zoning of buildings. Physical security of information within a business unit or building zone is the responsibility of the Information Asset Owners, individual managers and staff who work within those areas.

The RPO must respond promptly to any building physical security issues that are brought to their attention by any member of staff (or visitors) to remove or reduce any information security risk. Any remaining risk must be reported by the RPO to the Performance & Information Governance Manager and the relevant Information Asset Owners / Managers. These staff must then report this through their management chain to their Service management team to be considered as part of the Highland Council's approach to risk management.

16.9 Information Governance Board (IGB)

The IGB has been created to oversee the management of The Highland Council Information Management Strategy and the implementation of this across the Council. The IGB is chaired by the Senior Information Risk Owner. There is an IM Lead Officer from each of the Services who will represent their Service on the Board. Each ECO is required to identify a member of their senior management team to act as IM Lead Officer for their Service.

The primary role of the IGB is to identify priorities for the implementation of Information Governance improvements and the strategic initiatives identified in the associated Strategies and Implementation Plans.

The IGB has a duty to consider and make recommendations to the Senior Management Team about information governance issues and influence strategy and policy development.

The work of the IGB in relation to information governance will ensure that the Council improves its Data Protection practice. Compliance with this Data Protection policy will be reported to the IGB.

16.10 Information Management Lead Officer

The IM Lead Officer is a senior representative from each Council Service that represents their Service on the Information Management Governance Board (IMGB) and provides a strategic lead for information management issues (including records management) within each Service.

The IM Lead Officer will be required to attend the monthly IMGB meetings, communicate and cascade information within their Service and ensure adoption of working practices that are consistent with IM Policy and Guidance.

IM Lead Officers will be supported in their role through information and guidance provided through the Information Management Governance Board. Operational Support will also be available from IM Link Officers that have been identified within their Service.

16.11 Customer Resolution and Improvement Team

The Customer Resolution and Improvement Team is key to the coordination of Data Subject rights requests. They act as the contact point for Service staff and for the Data Protection Officer and provide assistance to Service staff in responding to requests.

16.12 Internal Audit

The Council's Internal Audit function includes responsibility for auditing the adequacy of the Council's Information Management policies, procedures, internal procedures, their implementation and Corporate and Service compliance with these.

17. Staff Communication & Training

This policy and associated guidance will be made available to staff through the intranet and for others who are within the scope of the policy through The Highland Council website (www.highland.gov.uk).

As part of the core training, staff and any person handling Council information are provided with an online learning module that provides an introduction to the expectations the Council places on those handling information. This includes data protection as well as information security and records management issues that staff should be aware of.

All staff must complete the information management online learning module and managers must ensure that this has been completed by their staff and is part of their Employee Review & Development Plan.

Any other person handling Highland Council information must also complete this training. The relevant Information Asset Owners and Managers within the Council must ensure this takes place in relation to the data processing and contracts they have responsibility for.

18. Review

This policy will be reviewed on a regular basis and adapted appropriately to ensure that it continues to meet the business and service delivery requirements of the Highland Council as well as changes to legislation.

Appendix 1 – Conditions for processing personal data.

UK GDPR Article 6 – Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

   a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes; [Consent]

   b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; [Contract]

   c) processing is necessary for compliance with a legal obligation to which the controller is subject; [Legal obligation]

   d) processing is necessary in order to protect the vital interests of the data subject or of another natural person; [Vital interests]

   e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; [Legal authority]

   f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. [Legitimate interests]

Point (f) shall not apply to processing carried out by public authorities in the performance of their tasks.

UK GDPR Article 9 – Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

2. Paragraph 1 shall not apply if one of the following applies:

   a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where domestic law provides that the prohibition referred to in paragraph 1 may not be lifted by the data subject; [Explicit consent]

   b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised

by domestic law or a collective agreement pursuant to domestic law providing for appropriate safeguards for the fundamental rights and the interests of the data subject; [Employment and social security]

c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent; [Vital interests]

d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects; [Appropriate bodies]

e) processing relates to personal data which are manifestly made public by the data subject; [Published information]

f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; [Legal claims]

g) processing is necessary for reasons of substantial public interest, on the basis of domestic law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject; [Substantial public interest]

h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3; [Health and Social Care]

i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of domestic law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy; [Public Health]

j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on domestic law (as supplemented by section 19 of the 2018 Act) which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject. [Archiving and research]

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the

responsibility of a professional subject to the obligation of professional secrecy under domestic law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under domestic law or rules established by national competent bodies.

3A. In paragraph 3, 'national competent bodies' means competent bodies of the United Kingdom or a part of the United Kingdom.

DPA 2018 Part 3, Section 31 – The law enforcement purposes

For the purposes of this Part, "the law enforcement purposes" are the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security.