Highland Council
Data Protection Policy

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 Draft	07/04/2016	Miles Watters	Amendment of Sections 7 and 8 to reflect Internal Audit findings

Document Authors

Miles Watters: Freedom of Information & Data Protection Manager

Distribution

Name	Role	Reason
	Resources Committee	Approval
Michelle Morris	Depute Chief Executive & Director of Corporate Development	Review and acceptance
	Information Management Governance Board	Review and acceptance
Vicki Nairn	Head of Digital Transformation	Review and acceptance
Kate Lackie	Business Manager	Review and acceptance
Philip Mallard	Information & Records Manager	Review

2. Introduction

The Highland Council is fully committed to compliance with the requirements of the Data Protection Act 1998. 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 the Act.

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. In addition, it may be required by law to collect and use information in order to comply with the requirements of the Scottish Government. 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 Act 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 as set out in the Data Protection Act 1998.

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

Processing
The act defines processing as obtaining, holding, use or disclosure of personal data. This means that data which is held in a record store or computer file store is being processed whether the information is in use or not.

Conditions for processing
The Act provides conditions for the processing of any personal data. It also makes a distinction between “personal data” and “sensitive personal data”. Appendix 1 gives the conditions for processing as contained in Schedules 2 and 3 of the Act.

Personal data
Personal data is defined as data relating to a living individual who can be identified from:

- That data;

- That data and other information which is in the possession of, or is likely to come into the possession of the data controller and includes an 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.

Sensitive personal data

Sensitive personal data is defined as personal data consisting of information as to:

- Racial or ethnic origin;
- Political opinion;
- Religious or other beliefs;
- Trade union membership;
- Physical or mental health or condition;
- Sexual life;
- Criminal proceedings or convictions.

5. Handling of personal data

The Act stipulates that anyone processing personal data must comply with eight 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

Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met.

Staff must be aware of the reasons for which they process personal data and be able to explain this to the data subject. Where required, informed consent must be obtained from the data subject before data is processed.

5.2 Principle 2

Personal data shall be obtained only for one or more specified and lawful purposes and shall not be further processed in any manner incompatible with that purpose or those purposes.

Where possible, data subjects must be informed of all purposes for which the data will be used at the time of collection. Services must ensure that applications forms contain clear explanations of how data will be used.

5.3 Principle 3

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which it is processed.

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

Personal data shall be accurate and where necessary, kept up to date.

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

Personal data shall not be kept for longer than is necessary for that purpose or those purposes.

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

5.6 Principle 6

Personal data shall be processed in accordance with the rights of data subjects under the Act. These include:

- The right to be informed that processing is being undertaken;
- The right of access to one's personal information within the statutory 40 calendar days;
- The right to prevent processing in certain circumstances;
- The right to correct, rectify, block or erase information regarded as wrong information.

5.7 Principle 7

Personal data shall be kept secure i.e. protected by an appropriate degree of security.

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 will be encrypted.

5.8 Principle 8

Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of data protection.

The Council must bear this principle in mind when procuring ICT contracts. Steps must be taken to ensure that server farms and data warehouses are situated within the European Economic Area or other areas recognised by the European Commission.

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

- There is someone with specific responsibility for data protection in the organisation;
- 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;
- 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 Act.

6. Data Subject Access

Data Subjects have the right, under Section 7 of the Act, to request information which is held about themselves. The Council has a process for handling data subject access requests. Details of this procedure are provided on the Council's intranet.

Where a formal data subject access request is received it should be forwarded to the Data Protection Officer (see Section 13.7) to be logged on the Customer Relationship Management System. The Council has 40 calendar days to comply with a data subject access request. Council compliance with data subject access requirements will be reported to Senior Management on a regular basis.

7. Data Processing

The Data Protection Act draws a distinction between one data controller sharing personal data with another (see Section 8), and a data controller sharing data with its data processor. The Data Protection Act requires that a data controller using a data processor must ensure, in a written contract, that:

- the processor only acts on instructions from the data controller;

  and

- the processor has security in place that is equivalent to that imposed on the data controller by the seventh data protection principle.

Therefore a data processor involved in data sharing doesn't have any direct data protection responsibilities of its own; they are all imposed on it through its contract with the Council.

This requirement is addressed by Sections 35 and 40 of the Council's standard terms and conditions which relate to security and data protection respectively.

All contractors who are users of personal information supplied by the council will be required to confirm that they will abide by the requirements of the Act with regard to information supplied by the Council.

8. Data Sharing

The Data Protection Act 1998 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 or other servants or agents of the Council) in terms of the control of personal data. This will enable them to agree whether either a data sharing agreement or a data processing contract (see Section 7) 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 the justification 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 is a member of the Highland Data Sharing Partnership (HDSP) which controls data sharing between The Highland Council, Police Scotland, NHS Highland, Scottish Fire and Rescue Service, and Argyll and Bute Council.

The HDSP has agreed a policy for sharing information and has published procedures on how to share information between partner agencies appropriately. These procedures should be followed whenever data is being shared with organisations within the HDSP. It should be noted, however, that under the HDSP procedures, data sharing agreements are still required for regular sharing of data between partner agencies.

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

9. Privacy Impact Assessment

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. Privacy impact assessment is carried out prior to implementing new procedures or systems or making major changes to existing ones.

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 Information Commissioner has produced a handbook for privacy impact assessments.

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. Guidance on carrying out these assessments is available on the Council's intranet.

10. Breaches

Where breaches of data protection occur, it is important that the Council takes immediate steps to reduce the impact on those whose data is affected. Serious breaches must be reported to the Information Commissioner's Office.

All Security breaches must be reported to the ICT Service Desk (0800 731 2702) immediately. Where security breaches involve personal data, the Data Protection Officer (see Section 13.7) is informed and a data protection breach report is compiled. The breach report contains 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.

Once completed, breach reports are presented to the Chief Executive, who agrees required changes or improvements with the relevant Service Director and decides whether the breach is sufficiently serious to report to the Information Commissioner.

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.

11. Notification to the Information Commissioner

The Information Commissioner maintains a public register of data controllers. The Highland Council is registered as such (Registration Number Z5442561).

The Data Protection Act 1998 requires every data controller who is processing personal data, to notify and renew their notification, on an annual basis. Failure to do so is a criminal offence.

To this end Information Asset Owners are responsible for notifying and updating the Data Protection Officer of the processing of personal data, within their units.

The Information Management Governance Board will review the Council's entry in the data protection register annually, prior to notification to the Information Commissioner.

Any changes to the register must be notified to the Information Commissioner, within 28 days.

To this end, any changes made between reviews will be brought to the attention of the Data Protection Officer immediately.

Councillors are data controllers in their own right. The Data Protection Officer ensures all Councillors are registered and that their registrations are up to date.

12. Supporting Policies

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

- Information Management Strategy
- Information Management Policy
- Records Management Policy
- Records Retention & Disposal Policy
- Information Security & Assurance Policy
- ICT Acceptable Use Policy
- The Employee Guide to Data Protection and Code of Conduct for Councillors.

13. Roles and responsibilities

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

13.1 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 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.

13.2 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.

13.3 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.

13.4 Senior Information Risk Owner (SIRO)

The SIRO is the senior person responsible for management of information security risks and for reporting this to the Depute Chief Executive & Director of Corporate Development and the Highland Council Senior Management Team. The SIRO role is performed by the Head of Digital Transformation.

The Head of Digital Transformation is the corporate strategic owner of Information Security as a part of Information Management Strategy.

13.5 Security Management

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

13.6 Information & Records Manager

The Information & Records Manager is responsible for ensuring all Highland Council records are held within appropriate records management systems and structures. The Information & Records Manager is 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.

13.7 Data Protection Officer

The Data Protection Officer role is performed by the Freedom of Information & Data Protection Manager who is responsible for dealing with requests for information under the Data Protection Act 1998, for providing advice about data sharing, for reviewing privacy impact assessments and for reporting serious breaches to the Information Commissioners Office (ICO). The Data Protection Officer is also the contact for the Information Commissioner's Office, when complaints are being investigated.

The Information & Records Manager 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 Act 1998.

13.8 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 Senior Information & Security Officer 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. A list of all properties and RPOs is maintained on the Council's intranet.

13.9 Information Management Governance Board (IMGB)

The IMGB has been created to oversee the management of The Highland Council Information Management Strategy and the implementation of this across the Council. There is an IM Lead Officer from each of the services who will represent their service on the Board. Each Service Director is required to identify a member of their senior management team to act as IM Lead Officer for their service.

The IMGB is chaired by the Head of Digital Transformation as the corporate owner of Information Management Strategy and Policy and as SIRO (Senior Information Risk Owner).

The primary role of the IGMB is to identify priorities for the implementation of Information Management improvements and the strategic initiatives identified in the IM Strategy Implementation Plan.

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

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

13.10 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.

13.11 Information Management Link Officer

The IM Link Officer is a role that exists to provide support to the IM Lead Officer and the Corporate IM functions in the implementation of Information and Records Management which support good data protection practice.

13.12 Internal Audit

The Highland 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.

14. 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 and the relevant Information Asset Owners and Manager within the Council responsible for the contract must ensure this takes place.

15. 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.

Schedule 2 - Conditions relevant for purposes of the first principle: processing of any personal data

1The data subject has given his consent to the processing.

2The processing is necessary—
(a)for the performance of a contract to which the data subject is a party, or
(b)for the taking of steps at the request of the data subject with a view to entering into a contract.

3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4The processing is necessary in order to protect the vital interests of the data subject.

5The processing is necessary—
(a)for the administration of justice,
(b)for the exercise of any functions conferred on any person by or under any enactment,
(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department, or
(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

6(1)The processing is necessary for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, except where the processing is unwarranted in any particular case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.
(2)The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.

Schedule 3 - Conditions relevant for purposes of the first principle: processing of sensitive personal data

1The data subject has given his explicit consent to the processing of the personal data.

2(1)The processing is necessary for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

(2)The Secretary of State may by order—
(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3The processing is necessary—

(a)in order to protect the vital interests of the data subject or another person, in a case where—

(i)consent cannot be given by or on behalf of the data subject, or

(ii)the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b)in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

4The processing—

(a)is carried out in the course of its legitimate activities by any body or association which—

(i)is not established or conducted for profit, and

(ii)exists for political, philosophical, religious or trade-union purposes,

(b)is carried out with appropriate safeguards for the rights and freedoms of data subjects,

(c)relates only to individuals who either are members of the body or association or have regular contact with it in connection with its purposes, and

(d)does not involve disclosure of the personal data to a third party without the consent of the data subject.

5The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

6The processing—

(a)is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b)is necessary for the purpose of obtaining legal advice, or

(c)is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

7(1)The processing is necessary—

(a)for the administration of justice,

(b)for the exercise of any functions conferred on any person by or under an enactment, or

(c)for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

(2)The Secretary of State may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

8(1)The processing is necessary for medical purposes and is undertaken by—

(a)a health professional, or

(b)a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2)In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1)The processing—

(a)is of sensitive personal data consisting of information as to racial or ethnic origin,

(b)is necessary for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained, and

(c)is carried out with appropriate safeguards for the rights and freedoms of data subjects.

(2)The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10The personal data are processed in circumstances specified in an order made by the Secretary of State for the purposes of this paragraph.