Agenda item	**12.**
Report no	**RES/27/18**

HIGHLAND COUNCIL

Meeting: Corporate Resources Committee

Date: 24 May 2018

Report Title: **Data Protection Policy Review**

Report By: The Chief Executive

1. Purpose/Executive Summary

1.1 On 25th May 2018 the EU General Data Protection Regulation (GDPR) will become law within the United Kingdom. All organisations which are currently subject to the Data Protection Act 1998 (DPA) must comply with these regulations by that date.

1.2 The GDPR will replace the current DPA and is described as making current best practice into law. The GDPR is also intended to update the legislation to take account of changing technologies and the ways in which citizens now engage with organisations.

1.3 Many aspects of Data Protection will not change as a result of the legislation and much of the Council's day to day work will be largely unaffected. The legislation does, however, require a number of changes to be made and, as a result, the Council's Data Protection Policy has been updated to take account of the legislative changes. This report summarises the changes and describes the impact of the new Data Protection Legislation on the Council and Members.

2. Recommendations

2.1 Members are asked to agree the following recommendations:

1. Note the changes to Data Protection legislation;
2. Note the effect on the Council and Members;
3. Agree that Data Protection Impact Assessments are undertaken whenever changes are being considered which may affect the processing of personal data; and
4. Approve the updated Data Protection Policy.

3. Background

3.1. On 25th May 2018 the EU General Data Protection Regulation (GDPR) will become law within the United Kingdom. All organisations which are currently subject to the Data Protection Act 1998 (DPA) must comply with these regulations from that date. The GDPR will replace the current DPA and is described as making current best practice into law. The GDPR is also intended to update the legislation to take account of changing technologies and the ways in which citizens now engage with organisations.

3.2. The UK Government has also published a Data Protection Bill (UKDPB) which is at final stages of approval within the UK Parliament. This Bill serves a number of purposes: 1) dealing with local derogations within GDPR; 2) implementing the EU Law Enforcement Directive (data protection rules for agencies involved in law enforcement activity); 3) creating data protection rules for national security; and 4) addressing the role and powers of the Information Commissioner under the new legislation.

3.3. The UKDPB confirms that GDPR will remain in place once the UK leaves the EU.

3.4 Many of the GDPR's concepts and principles are the same as the current DPA. However, there are some new elements and significant enhancements. Some of the key changes that will be brought about by GDPR are:

- Increased territorial scope.
- Increased penalties - the GDPR affords the Information Commissioner's Office (ICO) greater powers to fine organisations. Fines will be up to 2% of annual turnover or €10million (whichever is higher) for some types of breach and 4% of annual turnover or €20million (whichever is higher) for others. However, the 2% or 4% will not apply to public authorities.
- Consent – conditions for consent have been strengthened, it must be feely given, specific, informed and explicit. It must also be as easy to withdraw consent as it is to give it.
- Breach notification – Data breaches must be notified to the ICO within 72 hours (unless the breach is unlikely to result in a risk to the rights and freedoms of an individual). The data subject must also be notified where there is a risk to their rights or freedoms. Failure to comply could lead to enforcement action.
- Right of access – this will now be free of charge under GDPR. (Currently known as a subject access request for which the data subject may be charged a fee). The deadline will be reduced to "1 month" instead of 40 calendar days and failure to comply could lead to enforcement action or fines. It will be possible to charge for repeated requests and to refuse to comply with requests that are unreasonable.
- Right to be forgotten – gives a data subject the right to have the data controller erase his/her personal data and cease further processing and administration of their data. The Council will have to respond to these requests and explain, by reference to legislation, why they are unable to cease processing in some cases.

- Data portability – the right for a data subject to receive personal data concerning them and for their data to be easily transferred between organisations, for example when changing an energy supplier. This only applies where the processing is based on consent and the processing is automatic.
- Data protection by design – at its core, privacy by design calls for the inclusion of data protection from the outset of the designing of systems and policies, rather than an addition. GDPR mandates that data protection impact assessments are carried out in certain circumstances but it is good practice to undertake impact assessments for all new systems and policies.
- Provision of services to children – If you offer an 'information society service' (i.e. target online services) to children, you will need to obtain consent from a parent or guardian to process the child's data. The Council will need to consider if this applies, for example, to GLOW and, if so, who is responsible for managing consents.
- Data Protection Officers (DPO) – the appointment of a DPO will be mandatory for public organisations such as the Council. Failure to do so could lead to enforcement action or a fine.
- Transparency – the Council will be required to publish details of the processing of personal data that it carries out. This must include a standard set of information for each purpose which uses personal data including the justification for doing so.

3.4. As a result of this legislation, the Council's Data Protection Policy has been reviewed and updated to reflect obligations which come into force in May 2018. The new draft (version 2.0) Data Protection Policy is provided in appendix 1.

4. Summary of changes

4.1. Throughout the policy references to the Data Protection Act 1998 have been replaced with Data Protection Legislation. This is because those parts of the Council which have an enforcement role or roles related to the Criminal Justice process are subject to Part 3 of the forthcoming UK Data Protection Act and are not subject to GDPR. The phrase Data Protection Legislation covers all Council processing of personal data.

4.2. <u>Section 3 - Statement of policy and scope</u>
While the Council will continue to comply with the principles of Data Protection, the new legislation introduces the principle of "data protection by design and default". The statement of policy and scope has been updated to reflect this new obligation.

4.3. <u>Section 4 - Glossary of terms</u>
The previous definitions have been replaced with the equivalents from the new legislation. Appendix 1 has been updated to provide the new conditions for processing under the new legislation.

4.4. <u>Section 5 - Handling of personal data</u>
The principles have been updated with the text from the new legislation. There are now only 6 principles but these are equivalent to those in the current legislation. The 2 principles which have been removed relate to data subjects' rights and transfers of data to countries outwith the EEA. While

these are no longer considered to be principles, the obligations in relation to these issues have increased and there are new sections in the policy to address them.

4.5. Section 6 - Data subjects' rights
Section 6 has been updated to address all of the rights which data subjects will have as a result of the legislation. Previously, this section only referred to the right of Access. Additional guidance will be available regarding the handling of these requests.

4.6. Section 7 - The right to be informed
This is a new section which sets out the requirement for providing privacy notices to data subjects when they first provide personal data for one of the Council's purposes.

4.7. Section 8 – Transfers to third countries
This is a new section which explains the rules which must be followed if personal data needs to be regularly transferred to a country which is not a member of the European Economic Area. This is known to affect some aspects of the Wipro contract and Google for Education.

4.8. Section 9 – Data processing agreements
The new legislation requires that data processing takes place under written instruction from the data controller. This section states the criteria that all data processing agreements must meet. This can be part of the main contract or a separate data processing agreement. Discussions are taking place with procurement about whether any existing contracts will have to be varied to meet these criteria.

4.9. Section 10 – Joint controllers
This new section reflects the requirements under the legislation, in the situation where two data controllers decide the purpose for which data is processed. Examples include the public space CCTV and, to some extent the Council's work with the DWP.

4.10. Section 12 – Data protection impact assessments
The section on privacy impact assessments has been updated to reflect the need for "data protection by design and default". Previously the expectation was that PIAs would be carried out for new projects and major changes which affected the processing of personal data. The legislation expects any processing to be in compliance with all principles and data protection impact assessments are a useful tool to assist.

Therefore, Data Protection Impact Assessments (DPIAs) must be carried out whenever changes are being considered which may affect the processing of personal data no matter what the scale of the initiative is. DPIAs will also be used for new projects and when carrying out data protection audits.

4.11. Section 13 – Breach notification
Changes to this section reflect the fact that the Council will have only 72 hours from discovering a breach to report it to the ICO. Guidance for staff will be available on the intranet.

4.12. Section 14 – Data protection fees
While it is no longer necessary to notify the ICO of data processing activities, fees are still required by law to fund the work of the ICO. The requirement for Councillors to pay these fees continues.

4.13. Section 16 – Roles and responsibilities
The role of the Data Protection Officer has been updated to reflect the requirements of the new legislation. This includes the tasks that the legislation specifies for the role.

The Customer Services Officer role has been added as section 16.12 as they will be key to the management of data subjects' rights requests.

5. Impact on Elected Members

5.1. As Data Controllers in their own right, Councillors must comply with GDPR and the Council's Data Protection Policy. Whilst it is not anticipated that the legislation will require Councillors to make many changes to the way they handle personal data, there are implications for their ways of working which are set out below.

5.2. Councillors should continue to ensure that they keep personal data secure and that the respect their constituents' right to privacy. The Data Protection Officer will continue to ensure that all Councillors are registered with the Information Commissioner and that the appropriate fees are paid.

5.3. One of the major changes that will need to be accommodated is for Councillors to ensure that, when they are provided with personal data by constituents, they discuss the ways in which they will use that personal data with them. If, for example the Councillor intends to share the information with council officers to assist with a complaint, the constituent should be informed and any concerns they have about the level of detail that will be provided can be addressed. The key to good data protection practice, is that the data subject should not be surprised or upset by their data being used for purposes they had not expected.

5.4. The other major change is that Councillors will need to comply with the requirement under Article 13 of GDPR to provide a privacy notice when they receive a constituent's personal data for the first time. An example privacy notice has been drafted and provided to members. It has been added to each member's page on the Council's web site in order that a link to the notice can be included in acknowledgement of any emails received which contain personal data. Paper versions can also be provided to ensure that the notice can be given constituents who contact Councillors in person or at surgeries. Members will also need to accommodate the new requirements in the course of speaking to constituents on the phone and guidance has also been developed for this.

5.5. The Council's Data Protection Officer is available to discuss any queries or concerns that Members may have regarding compliance with GDPR.

6. Implications

6.1 Resource – there will be resource implications arising from changes to data protection legislation related to the requirement to appoint a Data Protection Officer. It is anticipated that this will be met from the Chief Executive's Office budget. Work towards compliance has required the use of staff resources across the organisation and this will carry on being the case to ensure the Council continues to be compliant. The scale of fines available to the Information Commissioner could have a significant resource impact if the Council fails to comply.

6.2 Legal – the report describes the impact of changes to legislation and its implications for the Council.

6.3 Community (Equality, Poverty and Rural) – there are no implications.

6.4 Climate Change / Carbon Clever – there are no implications.

6.5 Risk – there is a risk that failure to comply could lead to financial penalties and reputational damage

6.6 Gaelic – there are no implications.

Author: Miles Watters, Freedom of Information & Data Protection Manager

Date: 14 May 2018

Background Papers:

1. Data Protection Policy Version 2.0

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

Document Authors

Miles Watters: Freedom of Information & Data Protection Manager

Distribution

Name	Role	Reason
	Resources Committee	Approval
Derek Yule	Depute Chief Executive and Director of Corporate Resources	Review and acceptance
	Information Management Governance Board	Review and acceptance
Steve Walsh	Head of People and ICT	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 EU General Data Protection Regulation (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 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 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; [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; [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; [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; [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; [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; [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.

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 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 (GDPR Articles 13 & 14; DPA Section 44) (see section 7)
- The right of access (GDPR Article 15; DPA Section 45)
- The right to rectification (GDPR Article 16; DPA Section 46)
- The right to erasure (GDPR Article 17; DPA Section 47 & 48)
- The right to restrict processing (GDPR Article 18; DPA Section 47 & 48)
- The right to data portability (GDPR Article 20)
- The right to object (GDPR Article 21)
- Rights in relation to automated decision making and profiling (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 to 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 doesn't 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 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 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 GDPR and the DPA put restrictions on the transfer of personal data to countries out with the European Economic Area ("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 an "adequacy decision" by the European Commission. Currently these countries are Andorra, Argentina, Canada (commercial organisations), Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland, Uruguay and the US (limited to the Privacy Shield framework).

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 European Commission
- 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 EEA 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 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 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.

12. Data Protection Impact Assessments

Article 25 of the 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.

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 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. However, the Council must also report all breaches to the Information Commissioner's Office within 72 hours of becoming aware of the breach.

All Security breaches must be reported to the ICT Service Desk (01463 253150) immediately. Where security breaches involve personal data, the Data Protection Officer must also be informed immediately and a data protection breach report must be 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 Service Director and the Depute Chief Executive and Director of Corporate Resources 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 as are all Councillors as they are considered to be data controllers in their own right. The Data Protection Officer manages the payment of all of these fees.

15. 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.

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 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. The SIRO role is performed by the Depute Chief Executive & Director of Corporate Resources.

The Head of People and ICT is the corporate strategic owner of Information Security as a

part of the Information Management Strategy.

16.5 Security Management

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

16.6 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.

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 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 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 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.

16.9 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 People and ICT as the corporate owner of Information Security as a part of the Information Management Strategy.

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.

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 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.

16.12 Customer Services Officer

The Customer Services Officer role 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.

16.13 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.

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.

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 Union or Member State law provide 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 Union or Member State law or a collective agreement pursuant to Member State 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 Union or Member State 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 Union or Member State 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 Union or Member State 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 Union or Member State 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. [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

Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

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.