



Data Protection Policy

Version 6.0, 26 March 2021

This is a controlled document. Whilst this document may be printed, the electronic version posted on the intranet is the controlled copy. Any printed copies of this document are not controlled. As a controlled document, this document should not be saved onto local or network drives but should always be accessed from the intranet.

LIVE
LEARN
WORK
INVEST
VISIT

Document Control

| | |
|----------------|---|
| Organisation | North Lanarkshire Council |
| Title | Data Protection Policy |
| Creator | Gerry Gardiner |
| Owner | Senior Information Risk Officer |
| Subject | Governance of Council Information Assets |
| Classification | OFFICIAL |
| Identifier | 20210326 Data Protection Policy Version 6.0 |
| Date Issued | 4 June 2021 |

Revision History

| Revision | Originator | Date of revision | Revision Description |
|----------|----------------|------------------|--|
| 1.0 | Gerry Gardiner | 22.02.2013 | Following consultation with DGB |
| 2.0 | Gerry Gardiner | 04.07.2014 | Following consultation with DGB |
| 3.0 | Gerry Gardiner | 15.11.2016 | Bi-Annual Review |
| 4.0 | Gerry Gardiner | 10.05.2018 | To reflect the UK GDPR & DPA 18 |
| 5.0 | Paul Corrigan | 30.04.2020 | Bi-Annual Review incorporating feedback from DGB and DMT |
| 6.0 | Paul Corrigan | 26.03.2021 | Bi-Annual Review |

Document Approvals

| Sponsor Approval | Revision No. | Date |
|---|--------------|------------|
| Policy and Resources (F&CS) Sub Committee | 1.0 | 14.03.2013 |
| Policy and Resources (F&CS) Sub Committee | 2.0 | 16.09.2014 |
| Policy and Resources Committee | 3.0 | 21.06.2017 |
| Policy and Resources Committee | 4.0 | 07.06.2019 |
| Policy and Strategy Committee | 5.0 | 11.06.2020 |
| Policy and Strategy Committee | 6.0 | 03.06.2021 |

Document distribution and communication

This document will be made available to All Users. It will be published on the corporate intranet. Staff will be informed by periodic staff notices and induction information.

Contents

| | |
|--|-----------|
| 1. Introduction | 4 |
| 2. Information Risk | 4 |
| 2.1 Senior Information Risk Owner (SIRO) | 4 |
| 3. Data Protection | 4 |
| 4. Scope of this Policy | 5 |
| 4. Personal Data | 5 |
| 5. The Data Protection (DP) Principles | 6 |
| 7. Discharging our Responsibilities | 7 |
| 7.1 The Controller | 7 |
| 7.2 The Data Protection Officer (DPO) | 11 |
| 7.3 The Chief Executive and Executive Directors | 11 |
| 7.4 Business Managers | 12 |
| 7.5 All Users | 13 |
| 8. Privacy by Design and Data Protection Impact Assessments.(“DPIAs”) | 13 |
| 9. Data Protection Incidents/Breaches | 14 |
| 10. Data Protection Fee | 14 |
| 11. Documentation of processing activities | 14 |
| 12. Giving Information to other Departments and Third Parties | 15 |
| 13. Data Sharing | 15 |
| 14. Rights of Individuals | 16 |
| 15. Review and Revision | 17 |
| Appendix A: Glossary of Terms | 18 |
| Appendix 1 : Data Protection Impact Assessment Guidance and Template | 19 |
| Appendix 2 : Data Protection Breach And Incident Management Protocol | 31 |

1. Introduction

North Lanarkshire Council (“The Council”) provides a wide range of services for people who live or work in North Lanarkshire, who invest in North Lanarkshire and who visit North Lanarkshire. The Council also works in partnership with a range of public sector, commercial and voluntary sector organisations to provide services and support.

To deliver services effectively the Council needs to collect, process and hold large volumes of information relating to organisations and individuals.

2. Information Risk

The collation and holding of information of any nature creates a risk of information falling into the hands of third parties or misuse of the information. To manage those risks the Council has in place a number of policies. These are listed in the information governance policy framework document.

Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. The Council is exposed to potential fines of up to 20 million Euros (approximately £18 million) or 4% of its total annual turnover, whichever is higher and depending on the breach, for failure to comply with data protection law.

2.1 Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner (SIRO) is Head of Business Solutions. The SIRO’s duty is in respect of all information collected, held and processed by the Council. The SIRO is not a position prescribed or regulated by legislation. It is a position recommended by the Information Commissioner. The SIRO is responsible for:-

- (a) overall information risk and he/she will provide written advice on a regular basis to the Chief Executive on internal control and performance in respect of information risk;
- (b) assessing the impact of information risks on the Council and how the risks may be managed ensuring arrangements are put in place to mitigate risks. He/she will implement and lead information risk and management processes within the Council; and
- (c) advising the Corporate Management Team on effectiveness of information risk management across the Council.

3. Data Protection

As explained in 2 above, to deliver services effectively the Council needs to collect, process and hold large volumes of information which includes personal information (personal data) relating to current, past and prospective customers, clients, employees, workers, elected members, suppliers and contractors.

In addition, it may from time to time be required by law to process personal information to comply with the requirements of government departments and other public agencies. There are also instances where we process personal data for contractors and arms' length external organisations and third parties process Council information which includes personal data.

The UK General Data Protection Regulation (the "UK GDPR") sitting alongside the Data Protection Act 2018 (the "Act") make provision for how personal data (information) about living individuals in any form including paper and electronic must be collected, processed and held. They impose restrictions on how the Council may process personal data, and a breach of the Data Protection Laws could give rise to criminal and civil sanctions, including fines, as well as adverse publicity.

The legislation provides also that (i) special categories of personal data (i.e. data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and the processing of genetic data, biometric data, data concerning health, sex life or sexual orientation) and (ii) personal data relating to criminal offences and convictions shall only be collected and/or processed for certain specific lawful purposes. The Council can only process special categories of data and personal data relating to criminal offences and convictions where certain additional conditions apply. The Council has produced an appropriate policy document for such processing. For details of conditions for processing special categories of personal data see Article 9 of the UK GDPR and Schedule 1 of the Act. For details of conditions for processing personal data relating to criminal offences and convictions see Article 10 of the UK GDPR and Schedule 1 of the Act.

4. Scope of this Policy

This policy is applicable to all personal data held by the Council whether in manual format via Council information technology systems accessed either on Council premises or via mobile or home-working equipment. Personal data held on removable devices and other portable media is also covered by this policy.

The policy applies to all employees, workers, elected members, clients, suppliers, third party contractors and any other individuals or organisations who access Council information.

This policy is not part of the contract of employment and the Council may amend it at any time. However, it is a condition of employment that employees and others who obtain, handle, process, transport, store and otherwise process personal data will adhere to the rules of the policy. Any breach of the policy by an employee will be taken seriously and may result in disciplinary action.

Elected members are required, in respect of their use of data, to comply with their obligations as set out in paragraphs 3.16 and 3.17 of the Councillors' Code of Conduct and paragraphs 25 to 33 of the associated Guidance. In particular, members need to be aware of the potential for personal liability under the relevant legislation, in respect of both criminal and civil court proceedings as well as the imposition of fines by the Information Commissioner, as set out in paragraph 26 of the Guidance, together with the specific rules set out in paragraph 33.

Guidance to organisations on the UK GDPR is available from the Information Commissioner's Office at <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

5. Personal Data

This policy adopts the definition of personal data contained in the UK GDPR. Personal data is any information relating to an identified or identifiable natural person who can be directly or indirectly identified in particular by reference to an identifier.

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data.

Personal data that has been de-identified, encrypted or pseudonymised but can be used to re-identify a person remains personal data.

Personal data that has been rendered anonymous in such a way that the individual is not or no longer identifiable is no longer considered personal data. For data to be truly anonymised, the anonymisation must be irreversible.

Examples of personal data include a name and surname; a home address; an email address such as name.surname@company.com; an identification card number; CCTV images of an individual; location data (for example the location data function on a mobile phone); an Internet Protocol (IP) address; or a cookie ID.

The following are examples of data which are not considered to be personal data: a company registration number; an email address such as info@company.com; and anonymised data.

6. The Data Protection (DP) Principles

The UK GDPR requires organisations (like the Council) which handle personal data to collect, process and hold personal and confidential information securely and responsibly. This includes destroying information safely when it is no longer required.

The UK GDPR sets out the following key principles:

- First Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**).
- Second Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner incompatible with those purposes (**'purpose limitation'**).
- Third Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**).

- Fourth 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 are erased or rectified without delay (**'accuracy'**).
- Fifth 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 (**'storage limitation'**).
- Sixth 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 (**'integrity and confidentiality'**).

The Council is also responsible for, and must be able to demonstrate compliance with the Principles (**'accountability'**).

7. Discharging our Responsibilities

7.1 The Controller

In terms of the legislation, the Council will normally be the Data Controller. In some cases the Council may be acting as a Joint Data Controller in conjunction with another organisation. In some circumstances the Council may be acting as a data processor, for example, where it is providing services to an external or arms length organisation and is processing information of which that organisation is data controller and under their instruction in connection with provision of that service. To ensure compliance with the data protection principles, the Council will:

- a) Observe fully conditions regarding the lawful, fair and transparent collection and use of data.
- b) Meet its obligations to specify the purposes for which data is used.
- c) Collect and process appropriate data and only to the extent that it is required to fulfil operational needs or to comply with any legal requirements.
- d) Ensure the accuracy of the data used.
- e) Put in place arrangements to determine the length of time the data is held.
- f) Take appropriate measures to keep the data secure.

7.1.1 Lawful, Fair and Transparent Obtaining and Processing

The Council may only collect, process and share personal data fairly and lawfully and for specified purposes. The law restricts our actions regarding personal data to specified lawful purposes. These restrictions are not intended to prevent processing, but ensure that we process personal data fairly, lawfully and without adversely affecting the data subject.

It is essential that the legal ground ("lawful basis") being relied on for each processing activity is identified and documented.

The lawful bases for processing personal information are as follows. At least one of these must apply when you process personal data:

- (a) Consent – the individual has given clear consent for you to process their data for a specific purpose.
- (b) Contract – the processing is necessary for a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract.
- (c) Legal obligation – the processing is necessary for you to comply with the law (not including contractual obligation).
- (d) Vital interests – the processing is necessary to protect someone’s life.
- (e) Public task – the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law
- (f) Legitimate interests – the processing is necessary for your legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual’s personal data which overrides those legitimate interests. (This cannot apply if you are a public authority processing data to perform your official tasks).

For the majority of processing of personal data carried out by the Council the public task condition will be the appropriate lawful basis, however, it is very important that the appropriate lawful basis or bases are identified at the outset of processing activity and these will vary depending on the nature and circumstances of the processing in question.

For processing of “special category” data, a further additional lawful basis for processing requires to be satisfied. Special category data under data protection law relates to information about an individual’s race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (for ID purposes), health, sex life or sexual orientation.

There are extensive lawful bases within Schedule 1 of the Data Protection Act for processing in relation to special categories of personal data and data relating to criminal convictions. Advice should be sought from Legal Services in relation to proposed processing of such data.

The Council will be clear when telling people how their personal information will be used. This requirement to tell people will always apply, no matter how the information is gathered (for example, paper forms, email, surface mail correspondence, web data collection forms, or any other method). We must say clearly in all of these methods how we will process people’s personal information.

This should principally be achieved by the use of privacy notices. Privacy notices are a legal requirement. They inform data subjects about the collection and use of their personal data. This relates to the requirement under the legislation that processing of personal data should be transparent. Privacy notices should provide individuals with information about our purposes for processing their personal data, how long their data may be retained and with whom it may be shared. This information should be available to individuals at the point of collection of their data. The Council’s Privacy Notice can be found at <https://www.northlanarkshire.gov.uk/index.aspx?articleid=15003>.

Services should develop their own privacy notices to provide more specific information in relation to particular categories of processing of personal data in

relation to their functions. Privacy notices should be regularly reviewed and developed to ensure that they provide accurate and adequate information about the Council's processing activity.

Consent

In many cases the Council may process personal information without the consent of the data subject where this is required or permitted by law. However, the Council will ask for an individual's "informed consent" if this is needed (the individual must understand what their information will be used for and how it will be shared and stored) (see first DP Principle). Unless the Council can rely on another legal basis of processing, explicit consent will be required for processing special categories of personal data.

An individual consents to processing of their personal data if they indicate agreement clearly either by a statement or positive action to the processing. Consent requires affirmative action so silence, pre-ticked boxes or inactivity are unlikely to be sufficient. The individual may be asked to sign or to tick a box to give their consent. If consent is given in a document which deals with other matters, then the consent must be kept separate from those other matters.

Individuals must be easily able to withdraw consent to processing at any time and withdrawal must be promptly acted upon. Consent will need to be refreshed if the Council intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.

The Council will need to evidence consent captured and keep records of all consents so that we can demonstrate compliance with consent requirements.

7.1.2 Purpose limitation

Personal data must be collected only for specified, explicit and legitimate purposes. It must not be further processed in any manner incompatible with those purposes. The Council cannot use personal data for new, different or incompatible purposes from those disclosed when it was first obtained, unless it has informed the individual of the new purposes and they have consented where necessary.

7.1.3 Data minimisation

Personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed. The Council may only process personal data when required to do so in performance of its duties. The Council cannot process personal data for any unrelated purposes.

The Council will not collect excessive data. The Council will ensure that any personal data collected is adequate and relevant for the intended purposes.

When Personal Data is no longer needed for specified purposes, it should be deleted or anonymised in accordance with the Council's data retention guidelines.

7.1.4 Accuracy

The Council must make sure that all personal information that it holds is accurate and, where necessary up to date (fourth DP Principle). Information should be reviewed regularly and service managers must have procedures in place to make sure that inaccurate or out of date information is updated. Information which the Council no longer needs to hold must be destroyed in line with the Council's guidelines on Information Security.

7.1.5 Storage limitation

Personal data must not be kept in an identifiable form for longer than is necessary for the purposes for which the data is processed. The Council must not keep personal data in a form which permits the identification of individuals for longer than needed for the legitimate business purpose or purposes for which we originally collected it, including for the purpose of satisfying any legal, accounting or reporting requirements.

The Council will maintain retention policies and procedures to ensure personal data is deleted after a reasonable time for the purposes for which it was being held, unless a law requires such data to be kept for a minimum time.

The Council will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all the Council's applicable records retention schedules and policies. This includes requiring third parties to delete such data where applicable.

Individuals will be informed of the period for which data is stored and how that period is determined.

7.1.6 Security, Integrity and Confidentiality

Personal data must be secured by appropriate technical and organisational measures against unauthorised or unlawful processing, and against accidental loss, destruction or damage. We will continue to develop, implement and maintain safeguards appropriate to our size, scope and business, our available resources, the amount of personal data that we own or maintain on behalf of others and identified risks (including use of encryption and pseudonymisation where applicable). We will regularly evaluate and test the effectiveness of those safeguards to ensure security of our processing of personal data.

Personal data may only be transferred to third party service providers who agree to comply with the policies and procedures required by the Council and who agree to put adequate measures in place, as requested.

The confidentiality, integrity and availability of personal data must be maintained, i.e.

- **Confidentiality:** only people who have a need to know and are authorised to use the personal data can access it.
- **Integrity:** personal data is accurate and suitable for the purpose for which it is processed.

- **Availability:** authorised users are able to access personal data when they need it for authorised purposes.

7.1.7 Data Processors

The law requires the Council to put in place a written contract with each third party data processor, which contract must meet specific minimum requirements, including procedures and policies to maintain the security of all personal data from the point of collection to the point of destruction. Personal data may only be transferred to a third party data processor if the processor agrees in writing to comply with those minimum requirements.

7.1.8 ICO Assessments, Audits, Investigations and Action

The Council must co-operate with any data protection assessment, audit or investigation carried out or action taken by the Office of the Information Commissioner (ICO). Everyone subject to this policy must assist with any such assessment, audit, investigation or action as required by the ICO and / or the Council.

7.2 The Data Protection Officer (“DPO”)

The Council is required to appoint a DPO. The DPO is currently the Head of Service for Legal and Democratic Solutions. The DPO’s responsibility is in respect of personal data, collected, held and processed by the Council. The DPO will be involved, properly and in a timely manner, in all issues which relate to the protection of personal data.

The DPO’s responsibilities include:-

- (a) ensuring that the Council complies with the Data Protection Laws.
- (b) ensuring the Council and Council staff are fully informed of their own legal responsibilities and training of staff.
- (c) Developing and managing the Council’s Data Protection Policy, including development, implementation and enforcement of this policy and Data Protection procedures.
- (d) reporting on the Council’s compliance with the Data Protection Laws to the SIRO on a six monthly basis.
- (e) ensuring that necessary arrangements are in place for dealing where appropriate with subject access requests that relate to more than one service of the Council.
- (f) to provide advice where requested as regards data protection impact assessments and monitor their performance;
- (g) co-operating with the ICO.
- (h) acting as a point of contact for the ICO and consulting with the ICO as required.

7.3 The Chief Executive and Executive Directors

The Chief Executive and each Executive Director's responsibilities include:-

- (a) ensuring that the information under their control is collected, processed and held in accordance with this policy and the Data Protection Laws.
- (b) nominating lead contacts for data protection responsibility within their Services to the DPO; and immediately reporting changes of contact details to the DPO.
- (c) ensuring that necessary arrangements, including nominated officers, are in place to deal with subject access requests (see paragraph 13).
- (d) identifying and documenting all categories of personal information held within their service.
- (e) identifying and documenting all processing applied to that personal information.
- (f) identifying and documenting how long personal information needs to be held within each Service.
- (g) ensuring that necessary arrangements are in place within their Service for the secure disposal of personal data.
- (h) implementing procedures for the secure destruction of any personal information immediately when the Council no longer needs to keep it.
- (i) implementing arrangements and procedures as necessary for the safekeeping and preservation of all personal information held by their Services and ensuring that no one can get unlawful access to personal information that is held.
- (j) issuing instructions and implementing procedures to make sure that every person who has access to personal information held by their Service makes use of that information only for the purposes for which that information is held.
- (k) ensuring that all processing of personal information complies fully with all the provisions of the Data Protection Laws and this policy.

7.4 Business Managers

Business managers' responsibilities include:-

- (a) ensuring that employees and workers know what they have to do under the Data Protection Laws, ensuring that their staff are trained in data protection and confirming to the DPO when appropriate training has been undertaken by employees and maintaining records of training;
- (b) ensuring that disciplinary action up to the point of dismissal is taken where an employee or worker has deliberately breached the terms of the Data Protection Laws or this policy or of any of the Council's own procedures;

- (c) ensuring employees and workers know that they could face criminal proceedings if they deliberately or recklessly destroy information, obtain information or disclose it unlawfully;
- (d) ensuring that all personal information held is accurate and up to date; and
- (e) determining whether a Data Privacy Impact Assessment (“DPIA”) needs to be undertaken and, if so, putting in place appropriate arrangements to ensure that such a DPIA is undertaken and completed.

7.5 All Users

All Users must:

- (a) observe and comply with the Data Protection principles.
- (b) ensure that personal information is properly protected at all times. This requires continued compliance with the Data Protection Laws, this policy and all other Council information policies, procedures and guidance.
- (c) report any observed or suspected breach of this data protection policy or related information procedure and guidance (in accordance with the protocol set out in Appendix 2 to this policy).
- (d) ensure that individual archives, or any personal records they hold, are not kept when they are no longer required.

8. Privacy by Design and Data Privacy Impact Assessments (“DPIAs”)

We are required to implement Privacy by Design measures when processing personal data by implementing appropriate technical and organisational measures (like pseudonymisation) in an effective manner, to ensure compliance with data privacy principles. Pseudonymisation describes removing or replacing information within data set which identifies an individual.

Users must assess what privacy by design measures can be implemented on all programs/systems/processes that process personal data by taking into account the following:

- (a) the state of the art;
- (b) the cost of implementation;
- (c) the nature, scope, context and purposes of processing; and
- (d) the risks of varying likelihood and severity for rights and freedoms of data subjects posed by the processing.

The Council must also conduct DPIAs in respect to high risk processing.

Services should conduct a DPIA (and discuss the findings with the DPO) when implementing major system or business change programs involving the processing of personal data including:

- (a) use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- (b) automated processing including profiling and automated decision making;
- (c) large scale processing of special categories of data; and
- (d) large scale, systematic monitoring of a publicly accessible area.

A DPIA must include:

- (a) a description of the processing, its purposes and the Council's legitimate interests, if appropriate;
- (b) an assessment of the necessity and proportionality of the processing in relation to its purpose;
- (c) an assessment of the risk to individuals; and
- (d) the risk mitigation measures in place and demonstration of compliance.

The DPO is responsible for producing guidance on DPIAs and reviewing the guidance every alternate year commencing October 2012. (The current template and guidance and guidelines are contained in Appendix 1 of this policy, this guidance is regularly reviewed and updated and the up to date versions can be found on connect [DPIA Template](#) [DPIA Guidance](#)).

9. Data Protection Incidents/Breaches

The UK GDPR requires data controllers to keep a written record of data breaches, near misses or incidents. This is kept by the Council's DPO. Where any breach is assessed as resulting in a risk to the rights and freedoms of the individual(s) affected there is a requirement to notify the ICO of the breach. Where the breach is likely to result in a "high risk" to the rights and freedoms of affected individuals the UK GDPR requires that the individual(s) is/are informed without undue delay.

All incidents must be reported, whether or not the incident results in a breach of the Data Protection Laws and/or actual damage or loss to any person, to the DPO in accordance with the protocol in Appendix 2 to this policy. The DPO will take appropriate action in respect of the incident, in accordance with the said protocol. ("Incidents" are defined/explained in Appendix 2).

10. Data Protection Fee

It is the responsibility of the DPO to ensure payment of the annual data protection fee to the ICO and to provide all information required by the ICO when doing so.

11. Documentation of processing activities

The Council must document and maintain a written record of its data processing activities.

The DPO is responsible for ensuring that all categories of personal information and data subjects held by the Council are documented, including the uses to which the information is put, the categories of recipients of the personal information, details of transfers to third countries (including the transfer mechanism safeguards in place), the period for which the information will be held and a description of the technical and organisational measures in place to keep the information secure.

To enable the documentation to be kept up to date at all times, it is the responsibility of the Chief Executive and each Executive Director to advise the DPO immediately of:

- a) any new categories of information or data subjects held in his/her service.
- b) any changes in the uses to which his/her service is putting any personal information his/her service holds.
- c) any categories of personal information or data subjects which are no longer held by his/her service.
- d) any changes in categories of recipients of personal information held in his/her service.
- e) any changes in the transfer of personal information to third countries (including the transfer mechanism safeguards) in his/her service.
- f) any changes in the retention periods for personal information held in his/her service.
- g) any changes in the technical and organisational measures in place to keep information secure in his/her service.

12. Giving Information to other Departments and Third Parties

The Council must protect against processing personal information unlawfully. In most cases personal information can only be shared between council services and/or third parties where the individual concerned knows that such sharing may happen and where the processing complies with the Data Protection Principles. The first Data Protection Principle states that personal information shall be processed fairly, lawfully and in a transparent manner.

Where a request for personal information is received from a third party, the identity of the requester and the need for the information must be known before consideration is given to providing it. Personal information can be given to the police or the procurator fiscal to help with a criminal investigation and to certain statutory authorities/agencies (e.g. DWP and HMRC). This only applies in certain circumstances, so such requests for disclosure must be made in writing, providing details of the data subject, reason for disclosure, name of requesting officer and

certification by a senior officer. A record must be kept of all such disclosures by services and a report made available to the DPO immediately upon his request.

In all cases, if there are any concerns at all about an enquirer or their enquiry, information must not be given out and the enquiry should be referred to the DPO.

13. Data Sharing

Generally the Council is not allowed to share personal data with third parties unless certain safeguards and contractual arrangements have been put in place.

Services and officers might be approached and asked if the Council will enter into a Data Sharing Agreement with another organisation. A Data Sharing Agreement addresses arrangements whereby one organisation shares personal data with another organisation.

The Council will only share personal data it holds with third parties if:

- (a) they have a need to know the information for the purposes of providing the contracted services;
- (b) sharing the personal data complies with the privacy notice provided to the data subject and, if required, the data subject's consent has been obtained;
- (c) the third party has agreed to comply with the required data security standards, policies and procedures and put adequate security measures in place;
- (d) the transfer complies with any applicable cross border transfer restrictions; and
- (e) a written contract that contains approved third party clauses has been obtained.

A statutory draft Data Sharing Code of Practice in respect of data sharing arrangements between organisations has been issued by the ICO under Section 121 of the Data Protection Act 2018 . The draft code can be found at https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf The draft code explains how the 2018 Act applies to the sharing of personal data. It provides practical advice to organisations that share personal data and covers systematic data sharing arrangements as well as *ad hoc* or one off requests to share personal data.

Data Sharing Agreements should be approved by the Business Manager for the Service concerned and the negotiation and adjustment of the necessary legal documentation should be referred to the DPO and the Head of Business for Legal and Democratic Solutions, who will hold the signed completed agreements. The DPO will hold a register of all Data Sharing Agreements entered into by the Council.

14. Rights of Individuals

The Council, elected members, employees, workers, suppliers and contractors must respect the rights of all individuals (data subjects), including employees and elected members. These include rights to:

- (a) receive certain information about the Council's processing activities;
- (b) request access to their personal data that we hold;
- (c) prevent our use of their personal data for direct marketing purposes;
- (d) ask us to erase personal data if it is no longer necessary in relation to the purposes for which it was collected or processed or to rectify inaccurate data or to complete incomplete data;
- (e) restrict processing in specific circumstances;
- (f) challenge processing which has been justified on the basis of our legitimate interests or in the public interest;
- (g) object to decisions based solely on automated processing, including profiling;
- (h) prevent processing that is likely to cause damage or distress to the data subject or anyone else;
- (i) where processing is based on consent, withdraw consent to processing at any time;
- (j) be notified of a personal data breach which is likely to result in high risk to their rights and freedoms;
- (k) make a complaint to the ICO; and
- (l) in limited circumstances, receive or ask for their personal data to be transferred to a third party in a structured, commonly used and machine readable format.

The identity of an individual requesting data under any of the rights listed above should be verified before disclosing any personal information.

15. Review and Revision

This policy will be reviewed whenever guidance or the law is changed but at a minimum every 24 months. Policy review will be undertaken by the Data Governance Board under the guidance of the Senior Information Risk Owner.

Appendix A: Glossary of Terms

| Term | Description |
|-----------------------------|---|
| The Act | Data Protection Act 2018 |
| All Users | All parties who have access to Council information including employees, elected members and third party contractors and any other individuals or organisations who access Council information. |
| Council Information | Council information includes data, records, paper and digital formats. |
| Controller | The people or organisations who determine the purposes for which, and the manner in which, any personal data is processed. They have a responsibility to establish practices and policies in line with the Data Protection Laws. The Council is the controller of all personal data used in its business. |
| Data Protection Laws | The UK GDPR and the Act |
| DPO | Data Protection Officer |
| DWP | Department of Work and Pensions |
| The UK GDPR | UK General Data Protection Regulation |
| HMRC | Her Majesty's Revenue & Customs |
| ICO | Office of the Information Commissioner |
| | |
| Personal Data | 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. |
| Processing | 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. |
| Processor | Any person who processes personal data on behalf of a controller such as the Council. Council employees are excluded from this definition but it could include suppliers which handle personal data on behalf of the Council, for example where the Council outsources IT, payroll, paper waste disposal & mail shot / marketing services. |
| SIRO | Senior Information Risk Owner. |

APPENDIX 1 This guidance is regularly reviewed and updated and the up to date version can be found on connect [DPIA Guidance](#)

North Lanarkshire Council Data Protection Impact Assessment Guidance

Introduction

What is a Data Protection Impact Assessment (DPIA)?

A DPIA is a process to help you to identify and minimise the data protection risks associated with a project. A DPIA is a method of analysing the processing of personal data¹ which will arise as part of the project in question. They help to ensure compliance with the requirements of data protection law and have a particular focus on the risks which any proposed processing of personal data may present to any affected individuals.

To assess the level of risk, consideration should be given to the likelihood and severity of any impact on individuals. This will clearly vary depending on the nature and extent of the processing connected with the project or initiative. A DPIA should include a clear description of potential risks and explanation of steps proposed to address or mitigate any such risks.

A DPIA serves to ensure compliance with the principles of General Data Protection Regulation EU 2016/679 ("the UK GDPR") and the Data Protection Act 2018 ("DPA"). The principles of the legislation are as follows, and proper completion of any DPIA should ensure that these principles are adequately addressed:

- **Principle (a) Lawfulness, fairness and transparency**
The DPIA should confirm the appropriate lawful basis for any proposed processing. The effect of proposed processing on individuals must be considered and the individuals have a clear understanding of how we will collect and use their data.
- **Principle (b) Purpose limitation**
Personal data should only be used for the purpose or purposes for which it was collected. The data can only be used for a new purpose if that is compatible with the original purpose, we obtain the consent of the data subject, or there is a clear basis in law for this additional processing.
- **Principle (c) Data minimisation**
Only data which is necessary for the purposes of the proposed project should be collected or used.
- **Principle (d) Accuracy**
Personal data collected or otherwise processed should be accurate. Any challenges to the accuracy of personal data collected or processed as part of the project should be assessed.
- **Principle (e) Storage Limitation**
Personal data should not be kept for longer than is necessary. Consideration should be given as part of the DPIA to how long personal data will require to be held for the purposes of the project and describe proposals for secure disposal of personal data which is no longer required. This should make reference, where appropriate, to the Council's retention schedule.
- **Principle (f) Integrity and confidentiality**

¹ personal data is information relating to living individuals who can be identified or who are identifiable directly from the information in question, or who can be indirectly identified from that information in combination with other information

You must ensure that the proposal incorporates appropriate security measures to protect the personal data collected or processed as part of the project.

- **Accountability**

Proper completion of a DPIA will address the accountability principle under the UK GDPR in that it will document that the other six principles described above have been appropriately considered.

When is a DPIA required?

A DPIA is required in advance of any type of processing of personal data that is likely to result in a “high risk” to individuals. The purpose of the DPIA is to screen for potential factors which may present such a risk.

Under the UK GDPR, a DPIA must be done for projects which:

- Use systematic and extensive profiling with significant consequences for individuals;
- Process special category or criminal offence data on a large scale (special category data includes data relating to race, ethnic origin, politics, religion, trade union membership, genetics, bio-metrics (for ID purposes), health, sex life or sexual orientation);
- Systematically monitor publicly accessible places on a large scale.

What does “high risk” mean?

The following types of activities are likely to indicate “high risk” processing:

- Evaluation or scoring exercises of individuals including profiling;
- Automated decision making with legal or similar significant effect;
- Systematic monitoring (as above)
- Processing of sensitive/special category data or data of a highly personal nature;
- Large scale data processing;
- Matching or combining of data sets;
- Data concerning vulnerable data subjects;
- Innovative use or application of new technological or organisational solutions;
- Where processing itself prevents the data subject from exercising a right, or using a service or a contract.

The Information Commissioner’s Officer (ICO), who regulates data protection law, also requires a DPIA to be completed where the project involves:

- Profiling or use of special category data to decide on access to services;
- Profiling of individuals on a large scale;
- Processing of bio-metric data e.g. fingerprints;
- Processing of genetic data;
- Collection of personal data from a source other than the data subject without providing them with a privacy notice (invisible processing);
- Tracking of individuals’ location or behaviour;
- Profiling of children or targeting them for marketing or online services;
- Processing of data that might endanger the individual’s physical health or safety in the event of a security breach.

Even where there is no particular indication of likely “high risk”, it is good practice to do a DPIA for any major new project involving the use of personal data.

Identifying and assessing risks

Carrying out a DPIA should be viewed as a tool to manage the risks that processing poses to the rights of individuals. To identify and assess risk you need to think about what impact this processing

could have on individuals and whether it could cause financial, emotional, or physical harm. Potential harm could include:-

- Identity theft or fraud
- Financial loss

| | | | | | | |
|-------------------|-------------------------|----------------------------------|----------------|-------------------|----------------|---------------------------------|
| Likelihood | 5 Almost Certain | 5 | 10 | 15 | 20 | 25 |
| | 4 Likely | 4 | 8 | 12 | 16 | 20 |
| | 3 Possible | 3 | 6 | 9 | 12 | 15 |
| | 2 Unlikely | 2 | 4 | 6 | 8 | 10 |
| | 1 Rare | 1 | 2 | 3 | 4 | 5 |
| | | 1 Insignificant | 2 Minor | 3 Moderate | 4 Major | 5 Catastrophic |
| | Impact | | | | | |

- Loss of confidentiality
- Discrimination
- Lost control of data
- Limitations to an individual's rights (not just their privacy rights)
- Reputational damage.

Once the risks have been identified, you should assess each one including sources of risk and the potential impact of each type of breach (e.g. loss of data, unauthorised access). You will need to objectively consider the likelihood and severity of the possible harm. Using a risk matrix like the one below may prove useful:

Mitigating Risks

Once the risks associated with the processing have been identified and assessed, consideration should be given to how each of those risks can be mitigated. Examples of steps that could be taken include:-

- Deciding not to collect certain types of data;
- Reducing the scope of the processing;
- Reducing retention periods;
- Taking additional technological security measures;
- Training staff to ensure risks are anticipated and managed;
- Anonymising or pseudonymising data where possible;
- Putting data sharing agreements in place;
- Using a different technology;
- Ensuring internal guidance and processes are in place to avoid risk;
- Putting privacy notices in place/changing existing privacy notices;
- Offering individuals the opportunity to opt out (where appropriate);
- Implementing new systems to help individuals to exercise their rights.

The mitigating measures for each risk should be recorded as well as whether each measure will reduce or eliminate the risk.

The role of the DPO

It is a requirement that the DPO is consulted regarding all DPIAs. The DPO will provide advice on whether the processing is compliant and review/advise on any mitigating measures that may be required.

If the advice of the DPO is not followed, the reasons for this should be recorded.

DPIAs should be submitted, prior to sign off, to the Data Protection Team at DataProtection@northlan.gov.uk.

Once the DPIA is complete

The outcomes of the DPIA should be integrated into project plans. You should identify any action points and who is responsible for implementing them. You can use the usual project-management process to ensure these are followed through.

The ongoing performance of the DPIA should be monitored. You may need to cycle through the process again before your plans are finalised.

If it is decided to accept a high risk, either because it is not possible to mitigate or because the costs of mitigation are too high, the ICO must be consulted before the processing begins. Advice should be sought from the Data Protection Team in these circumstances.

The DPIA should be kept under review. It may need to be repeated if there is a substantial change to the nature, scope, context or purposes of the processing.

The DPIA Screening template and DPIA template

The DPIA screening template and DPIA template contained within Appendices 1 and 2 of this guidance are designed to assist you in (a) deciding if a DPIA is required (or appropriate) and (b) carrying out a DPIA. The screening template should be completed in full as a first step to assess whether a full DPIA is required. At the end of the screening process you should document your decision as to whether a full DPIA is required and record clearly why you have made the decision. If the decision is that a DPIA is not required, you should retain the completed screening template as a record of that decision.

Supplementary guidance on how to fully answer the questions is provided within the templates.





Any further advice required can be sought from the Data Protection Team at DataProtection@northlan.gov.uk.

This template is regularly reviewed and updated and the up to date version can be found on [connect DPIA Template](#)
Data Protection Impact Assessment (DPIA)

Screening Template

You should complete this screening template at the outset of any new project, or if you are reviewing any existing arrangements where there is not an up-to-date DPIA in place. The purpose of completing this initial screening template is to help you identify whether or not you need to carry out a DPIA. You should refer to the DPIA Guidance document when completing this form.

If you need any parts of this form or the guidance clarified or explained further, please get in touch with the Data Protection Team at DataProtection@northlan.gov.uk

| Contact details | |
|--|---|
| Name of person completing this DPIA | |
| Name of team (if appropriate) | |
| Division | |
| Service | |
| Contact details |  <input style="width: 150px;" type="text"/>  <input style="width: 150px;" type="text"/> |
| Name of Senior Responsible Owner (if applicable) | |
| Contact details |  <input style="width: 150px;" type="text"/>  <input style="width: 150px;" type="text"/> |

| External partners - please provide details where project or activity is being developed jointly with another organisation(s) | |
|--|--|
| Name of organisation | |

Screening Questions

| |
|---|
| 1. Briefly describe what your project/activity aims to achieve and its scope. You may find it helpful to refer to other documents such as a project proposal, Project Initiation Document (PID) or Business Case. Please provide a hyperlink to these documents where applicable. |
| As part of consideration of the likelihood of processing of personal data presenting a "high risk" it is important to describe the scale of the project and, so far as possible, the extent of data subjects likely to be affected by the processing in question. If the project is particularly technical in nature, please try to describe the project in non-technical terms so far as possible. |
| 2. Does your project/activity collect or use personal data and how will it be used? |

| | |
|---|--|
| <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> | <p>If yes, list the personal data (e.g. e-mail address, phone number, National Insurance number). Describe why the personal data is needed and how you will use it. (e.g. Individuals will be contacted to participate in a survey) If no, then there is no need to complete a DPIA. You should keep this document as a record of the basis of your decision not to proceed with a DPIA.</p> <p>You should remember that personal data is information which either on its own, or in combination with other information, identifies a living individual. Therefore, if your project involves sharing information with another party, your decision as to whether the data constitutes personal data should take account of information that the other party may already hold.</p> |
| <p>3. Do you intend to collect sensitive data or personal data from people in vulnerable positions (e.g. children, elderly people, carers, ex-offenders)? Do you need to collect information about criminal convictions, or alleged criminal acts?</p> | |
| <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> | <p>If yes, identify and describe the data, and/or, describe why the individuals are in a vulnerable position.</p> <p>Sensitive data would include special category data and also highly personal information or information which could potentially compromise the privacy, safety or security of the individual e.g. financial or bank account information, National Insurance number or other personal identifiers.</p> <p>Whether or not a person is in a vulnerable position (for the purposes of this process) centres round their ability to freely consent or object to the processing of their personal data, or to understand the implications. This will include children (those under 13 years of age), people with disabilities that affect their capacity and some elderly people but it is not necessarily restricted to these groups.</p> |
| <p>4. Will your project/activity require you to get in direct contact with individuals in a way that could be seen as intrusive or 'cold'? (e.g. if people are not expecting to receive your call or e-mail, they may perceive it to be a 'cold' call.) What is the lawful basis for using this personal data?</p> | |
| <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> | <p>If yes, describe how you intend to get in touch with individuals.</p> <p>The requirement to process personal data fairly, transparently and for specified, limited purposes means that you should not be using an individual's personal data in a way that they would not expect. If a project would involve direct contact with individuals, you should consider whether this is covered by any existing privacy notice or whether you will need to provide them with this privacy information when you contact them.</p> |
| <p>5. Do you have an existing relationship with the individuals from whom you are collecting data? (e.g. people who receive home support services, business community representatives)</p> | |
| <p>Yes <input type="checkbox"/></p> <p>No <input type="checkbox"/></p> | |
| <p>6. Summarise why you identified the potential need for a DPIA</p> | |

Please refer to the DPIA guidance document for guidance on when a DPIA is required.

Next Steps

Once you have completed the form you should consider whether or not you require to proceed to carry out a DPIA. Guidance on when you are required by law to carry out a DPIA, or when it is good practice to carry one out, is provided in the DPIA guidance. If you decide that your project does not require a DPIA you should retain this document as a record of that decision. If you decide that a DPIA is required you should proceed to complete the sections below. If you require advice on whether or not a DPIA is required you should contact the Data Protection Team at DataProtection@northlan.gov.uk

Decision:

Proceed with DPIA

Do not proceed with DPIA

Reasons for decision:

Data Protection Impact Assessment (DPIA)

Where you have completed the screening template and decided to proceed with a full DPIA you should complete the remaining questions on this form.

If you need any the following questions clarified or explained further, please get in touch with the Data Protection Team for guidance at DataProtection@northlan.gov.uk

Please also refer to the separate DPIA Guidance document for further information. Supplementary guidance on how to answer particular questions is provided below, where appropriate.

7. Will you be using personal data in a 'new' way for this project/activity

8. What is the ultimate benefit of your project/activity? What are the benefits of processing the data – for the council and more broadly? What is the intended effect on individuals?

9. Where are you getting the personal data from? Describe the source of the data and how you will collect it. How many individuals are affected and what geographical area does the data cover?

10. What is the nature of the data and does it include special category or criminal offence data?

[Refer to guidance for definitions of special category and criminal offence data.](#)

11. Describe the nature of the processing. How much data will you be using and how will you use it? How often will you use the data and for how long will it be kept?

Describing the nature of the processing will involve consideration of a number of questions:-
How will the personal data be collected, stored and used?
Who will have access to it and who will it be shared with?
Will a data processor be used?
How long will the personal data be kept?

In terms of how long data will be kept, you should refer to the Council's retention schedule. If the project involves collecting new information not previously held by the Council you should consider whether there are any legal restrictions on how long to keep the information for, and if not, you should think about the business need to keep the information. You should not keep personal information indefinitely – in fact you should keep it for no longer than is necessary for the purpose for which you've collected it.

12. How will you ensure that personal data is kept secure at every stage of the project/activity and how will the data be deleted?

You should consult IT for guidance on appropriate information security measures for your project.

13. How will you ensure data quality and data minimisation and what measures will you take to ensure that processors comply?

Data quality refers to the accuracy of personal data. Data minimisation involves ensuring that only the minimum personal data necessary for the project will be processed.

The most likely measure to ensure processors comply, would be by entering into a data processor agreement containing appropriate terms. The Data Protection Team will be able to assist with the drafting of these agreements.

14. Are there any prior concerns or uncertainties around this type of processing? Is the processing novel in any way or are there any identified security flaws? Does the proposed method of processing present any identified risks which do not currently exist in any existing method of processing? Are there any issue of public concern that you should factor in? What is the current state of technology in this area? Are we signed up to any approved conduct or certification scheme that relates to this type of processing?

Technical advice should be sought from IT as required.

15. What is the nature of the council's relationship with the individuals? What information will you give to individuals and how will you support their rights? How much control do they have and would they expect us to use their data in this way?

Any processing of personal data must be carried out fairly – meaning it is not unduly detrimental, unexpected or misleading. It also must be carried out in a clear and transparent manner. You should consider how you plan to tell individuals about this processing - this can likely be achieved via an appropriate privacy notice, though further methods of communication may be required.

16. How and when will you consult with relevant stakeholders and seek their views? If it is not appropriate to do so, please justify why.

The UK GDPR requires you to consult with data subjects, or their representatives, where it is appropriate to do so i.e. unless there is a good reason not to. There are a variety of ways individuals can be consulted – a public consultation, targeted research, surveys sent to service users are some examples.

If a decision is made not to consult individuals, this should be documented and the reasons for not consulting them should also be recorded. Reasons for not consulting individuals might be that it will involve disproportionate effort, it is impractical or it would compromise commercial confidentiality.

If the DPIA decision differs from the views of the data subjects, the reasons why their views are being disregarded should be recorded.

17. Who else do you need to involve from within the council or externally? Do you plan to consult information security experts or any other experts?

If a data processor is involved it may also be appropriate to consult with them. They are required to assist and provide any necessary information, as part of their obligations as processors under the UK GDPR.

18. Who will the personal data be shared with during and after the project/activity? For example – will the data be shared with any other organisations?

If the project will involve routinely sharing personal data with third parties consideration should be given to whether a data sharing agreement is already in place, or if one is required. There is no legal requirement to have a data sharing agreement in place, however, if the project involves the regular sharing of personal information, then you should consider entering into a data sharing agreement. This will clarify and record the basis for the sharing of personal data and reduce the risks associated with disclosing personal data outwith the Council.

19. Will the data be shared outwith the European Economic Area?

The UK GDPR restricts the transfer of personal data to countries outside the EEA*, or international organisations. These restrictions apply to all transfers, no matter the size of transfer or how often they are carried out.

To determine whether data is being transferred outside the EEA, you should consider where any processors or organisations with whom data will be shared as part of this project are located. In addition to that, the location of any servers upon which data will be stored should be identified. If either an organisation, or a server, is not located within the EEA, advice should be sought from the Data Protection team at DataProtection@northlan.gov.uk.





*All countries in the European Union plus Iceland, Liechtenstein and Norway.
For further information see: <https://www.gov.uk/eu-eea>

20. If an external organisation or partner is involved, what recommendations has their Data Protection Officer given to mitigate the risks associated with this project/activity?

21. Does this processing activity achieve your purpose? Is there another way to achieve the same outcome?

Part of the DPIA process is considering whether the proposed processing of personal data is a necessary and proportionate means of achieving the desired outcome. If you can achieve the same outcome without processing personal data, for example, by using anonymised data sets, then you should not proceed with the processing.

22. External partners - please provide details where project or activity is being developed jointly with another organisation(s)

| | | | |
|---|---|--|---|
| Name of contact person in partner organisation | | | |
| Name of organisation | | | |
| Contact details |  | |  |
| Name of external organisation's Data Protection Officer | | | |
| Contact details |  | |  |

Identifying and Assessing Risks

Measures to Reduce Risks

Sign Off and Approval

Recording Outcomes

Please send a copy of the completed DPIA to the Data Protection Team at DataProtection@northlan.gov.uk.

DPO Comments / Approval

Reasons for decision:

APPENDIX 2

NORTH LANARKSHIRE COUNCIL

DATA PROTECTION BREACH AND INCIDENT MANAGEMENT PROTOCOL

1. Background to this Protocol

Every care is taken by North Lanarkshire Council (the "Council") to protect personal data and to avoid a personal data breach. In the unlikely event of personal data being lost, damaged, misused, altered, stolen or otherwise shared or accessed inappropriately it is vital that appropriate action is taken to minimise any associated risk as soon as possible.

For the purposes of this protocol,

- ***A personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; and***
- ***where an incident e.g. theft of an encrypted laptop or any other incident involving a loss / inappropriate sharing of personal data has occurred but there has been no adverse consequence as a result of the loss / inappropriate sharing, it will be constituted 'a near miss'.***

2. Reporting Personal Data Breaches

The Council is under an obligation to report certain types of personal data breach. For that reason it is essential for the Council to have an effective personal data breach reporting process in place to ensure that personal data breaches are detected and notified promptly accompanied by all necessary information.

- The Council must, without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the ICO if the data breach is likely to result in a risk to the rights and freedoms of individuals.
- If notification is not given within 72 hours, the Council must provide the ICO with an explanation for the delay.
- The Council must also inform affected individuals without undue delay if a personal data breach is likely to result in a high risk to the rights and freedoms of the individuals concerned.
- Failure by the Council to notify when required to do so could result in a fine of up to 10 million Euros or 2% of the Council's annual turnover. The ICO could also take other enforcement action.
- The Council's processors are required to notify the Council without undue delay after becoming aware of a personal data breach.

3. Purpose of this Protocol

This protocol sets out the procedure to be followed by all NLC officers, staff, elected members and third party contractors if a personal data breach takes place, or is believed to have taken place or where there has been 'a near miss'.

4. **Scope of this Protocol**

This protocol applies to all personal data held by or on behalf of NLC.

5. **Types of Breach**

A personal data breach is not limited to loss or theft of personal data. Data protection breaches could be caused by a number of factors. Some examples are:

- Loss or theft of data or equipment on which data is stored;
- Inappropriate access controls allowing unauthorised use;
- Sending personal data to the wrong person
- Equipment failure;
- Human error;
- Unforeseen circumstances such as fire or flood;
- Hacking, phone/email 'Phishing' and other 'social engineering' methods;
- 'Blagging' offences where information is obtained by deception;

6. **Immediate Mitigation / Recovery Actions**

- 6.1 The person who identifies a personal data breach or near miss (collectively referred to as an **"incident"**) must inform his / her Head of Service or their representative in accordance with any agreed reporting mechanism . If the incident occurs or is discovered outside normal working hours, this should be done as soon as is practicable.
- 6.2 The Head of Service/senior manager who is informed of the incident must ensure that arrangements are in place for the Data Protection Officer (the **"DPO"**) to be informed at the earliest opportunity. Where an incident relates to loss of data held electronically the Head of Business Solutions must also be informed by the Head of Service/senior manager.
- 6.3 If the person who identifies an incident is a Head of Service, he or she must make arrangements to inform the DPO as soon as possible.
- 6.4 The officer to whom an incident is reported must ascertain whether, if the incident is a personal data breach, the personal data breach is still occurring. If the personal data breach is still occurring, steps must be taken immediately to minimise its effect. An example might be to shut down a system, or to alert relevant staff.
- 6.5 The relevant Head of Service, or their representative, in consultation the DPO or their representative will also consider whether the police need to be informed. This would be appropriate where illegal activity is known or is believed to have occurred (including where there has been a theft or loss of a laptop or other mobile device) or where there is a risk that illegal activity might occur in the future.
- 6.6 If bank details have been lost / stolen, the Head of Financial Solutions must be contacted immediately to ensure that appropriate steps are taken to limit / contain loss or damage.

- 6.7 The relevant Head of Service or their representative must quickly take appropriate steps to recover any losses and limit the damage. Steps might include:
- a. Attempting to recover lost equipment;
 - b. Contacting other officers as appropriate, to ensure that he / she is prepared for any potentially inappropriate enquiries;
 - c. Contacting the Head of Strategic Communication so that he / she is prepared to handle any press enquiries;
 - d. The use of back-ups to restore lost / damaged / stolen data; and
 - e. If the incident includes any entry codes or passwords, then these codes must be changed immediately, and the relevant agencies and members of staff informed.

7. Investigation

In most cases, the next stage is for the relevant Head of Service or their representative to investigate the incident fully. They should ascertain whose data was involved in the incident, the potential effect on the data subject(s) and what further steps need to be taken to remedy the situation.

The investigation should consider the type of data, its sensitivity, what protections are in place (e.g. encryption), what has happened to the data, whether the data could be put to any illegal or inappropriate use, how many people are affected, what type of people have been affected (the public, suppliers etc.), what harm could come to those affected and whether there are wider consequences to the incident.

The investigation should be completed urgently and, wherever possible, within 48 hours of the incident being discovered / reported. A further review of the causes of the incident and recommendations for future improvements can be done once the incident has been resolved.

8. Accountability and Record of Incident

Irrespective of whether the Council is required to report a personal data breach, the Council will make and keep a record of incidents.

A clear written record should be made and maintained of the nature of the incident, its cause, its effects, the actions taken to mitigate it and the actions taken to try to prevent a recurrence of a similar incident. This information should be provided to the DPO as soon as possible by completion of the [Data Breach Notification document](#).

If the Council decides not to notify an incident, a justification for that decision should be documented. This should include reasons why the Council considers the incident is unlikely to result in a risk to individuals.

The DPO will retain a register of all incidents.

9. Notification

- 9.1 The ICO, affected individuals and others (such as the police and insurers) may need to be notified as part of the initial containment. However, the decision will normally be made once an investigation has taken place.

- 9.2 Where there is a likelihood of risk of harm to individuals, the ICO may require to be notified without undue delay and within the 72 hour period referred to above.
- 9.3 Where there is the likelihood of a high risk of harm to individuals, affected individuals may require to be notified without undue delay.
- 9.4 A decision whether to notify the ICO and affected individuals will be made by the DPO. Breaches will be considered on a case by case basis. The DPO will assess the risk that could result from the incident and should take account of the following criteria:
- (a) the type of breach;
 - (b) the nature, sensitivity, and volume of personal data;
 - (c) the ease of identification of individuals;
 - (d) the severity of consequences for individuals;
 - (e) the special characteristics of the individuals (such as children or vulnerable individuals);
 - (f) the number of affected individuals;
 - (g) the special characteristics of the Council.
- 9.5 The DPO will take account of the likelihood and potential severity of the impact on individuals. Knowing the likelihood and potential severity of the impact on the individual will help the DPO to determine whether notification is required to the ICO and, if necessary, to the individuals concerned.
- 9.6 An incident is likely to result in a high risk to individuals if it may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. Damage should be considered likely to occur if the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or security related measures.

10. Notification to the ICO

Where notification is required, at the very minimum the notification must

- (a) describe the nature of the personal data breach including where possible:
 - a. the categories and approximate number of individuals concerned; and
 - b. the categories and approximate number of personal data records concerned;
- (b) give the name and contact details of the DPO or other contact point where more information can be obtained;
- (c) describe the likely consequences of the personal data breach; and
- (d) describe the measures taken or proposed to be taken to deal with the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

If it is not possible to provide the information all at once, the information can be submitted in stages provided there is no delay in doing so.

11. Notification to individuals

- 11.1 The relevant Executive Director / Head of Service or their representative will notify individuals where appropriate. When notifying individuals, they should be provided with specific and clear advice on what they can do to protect themselves and what the service can and will do to help them. They should also give them the opportunity to make a formal complaint if they wish (see the Council's Complaints Procedure).
- 11.2 The notification must describe in clear and plain language the nature of the personal data breach and at the minimum:
- (a) give the name and contact details of the DPO or other contact point where more information can be obtained;
 - (b) describe the likely consequences of the personal data breach; and
 - (c) describe the measures taken or proposed to be taken to deal with the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
- 11.3 However, notification is not necessary if:
- (a) the Council has implemented appropriate technical and organisational protection measures, and those measures were in place, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption; or
 - (b) the Council has taken subsequent measures which ensure that the high risk to the rights and freedoms of individuals is no longer likely to materialise; or
 - (c) it would involve disproportionate effort provided that the Council instead issues a public communication (or something similar) whereby they are informed in an equally effective manner.

Even if individuals have not been informed, the ICO may require the Council to do so.

12. Review and Evaluation

Once the initial aftermath of the incident is over, the Head of Service or their representative should fully review both the causes of the breach and the effectiveness of the response to it. If systemic or ongoing problems are identified, then an action plan must be drawn up to put these right. If the incident warrants a disciplinary investigation, the manager leading the investigation should liaise where appropriate with the DPO and Head of Human Resources for advice and guidance.

13. Review

This protocol will be reviewed every other year commencing June 2014. It may also be reviewed following upon an incident, legislative changes, new case law or new guidance from a relevant agency.

14. Implementation

This protocol has immediate effect. All service managers should ensure that staff are aware of the Council's Data Protection Policy, this protocol and their requirements. This should be undertaken as part of induction and supervision.

If officers have any queries in relation to the procedure, they should discuss this with their line manager.