Data Protection Policy

Document Control

Organisation	CultureNL Ltd
Title	Data Protection Policy
Author	Fiona Hughes
Owner	Chief Executive
Identifier	Data Protection Policy v.1.0

Revision History

Version No.	Author	Date	Description
1.0	Fiona Hughes	May 2019	Modelled on North Lanarkshire Data Protection Policy v.4.0

Document Approvals

This policy is subject to approval by the Board of CultureNL Ltd.

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

CultureNL Ltd ("CultureNL") is the cultural trust, wholly owned by North Lanarkshire Council, providing cultural services for people who live or work in North Lanarkshire, who invest in North Lanarkshire and who visit North Lanarkshire. CultureNL also works in partnership with a range of public sector, commercial and voluntary sector organisations to provide services and support.

To deliver services effectively CultureNL 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 the risk of information falling unintentionally into the hands of third parties or the misuse of the information. To manage those risks CultureNL has adopted a number of policies. These are listed in the information governance policy framework document of North Lanarkshire Council and posted on the CultureNL intranet pages. Protecting the confidentiality and integrity of personal data is a critical responsibility that we take seriously at all times. CultureNL 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.

3. Data Protection

As explained in 2 above, to deliver services effectively CultureNL 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 where third parties process CultureNL information which includes personal data.

The General Data Protection Regulation (the "GDPR") and 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 CultureNL 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 bad 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. CultureNL can only process special categories of data and personal data relating to criminal offences and convictions where certain additional conditions apply. For details of conditions for processing special categories of personal data see Article 9 of the 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 GDPR and Schedule 1 of the Act.

4. Scope of this Policy

This policy is applicable to all personal data held by CultureNL whether in manual form and accessed on CultureNL premises or via CultureNL information technology systems accessed on CultureNL 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 CultureNL information.

This policy is not part of the contract of employment and CultureNL 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 will be taken seriously and may result in disciplinary action.

5. Personal Data

This policy adopts the definition of personal data contained in the 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; 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 GDPR requires organisations (like CultureNL) 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 GDPR sets outs 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 not 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’**).

CultureNL is also responsible for, and must be able to demonstrate compliance with the Principles (‘**accountability**’).

7. Discharging our Responsibilities

7.1 The Controller

Where, in terms of the legislation, CultureNL is the Controller, to ensure compliance with the data protection principles, CultureNL 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

CultureNL 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 and without adversely affecting the data subject.

It is essential that the legal ground being relied on for each processing activity is identified and documented.

CultureNL 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.

Consent

In many cases CultureNL may process personal information without consent where this is required or permitted by law. However, CultureNL 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 CultureNL can rely on another legal basis of processing, explicit consent will be required for processing special categories of personal data.

An individual consents to the 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 may need to be refreshed if CultureNL intends to process personal data for a different and incompatible purpose which was not disclosed when the individual first consented.

CultureNL 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. CultureNL cannot use personal data for new, different or incompatible purposes from that 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. CultureNL may only process personal data when performing its duties requires it. CultureNL cannot process personal data for any unrelated purposes.

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

You must ensure that when Personal Data is no longer needed for specified purposes, it is deleted or anonymised in accordance with the Company's data retention guidelines.

7.1.4 Accuracy

CultureNL 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 that CultureNL no longer needs to hold must be destroyed in line with CultureNL'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. CultureNL 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.

CultureNL 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.

CultureNL will take all reasonable steps to destroy or erase from our systems all personal data that we no longer require in accordance with all CultureNL'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 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 CultureNL 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 CultureNL 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 Assessments, Audits, Investigations and Action

CultureNL 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 CultureNL, North Lanarkshire Council or the ICO.

7.2 The Data Protection Officer (DPO)

CultureNL is required to appoint a DPO. The DPO is currently the Corporate Records Manager. The DPO's responsibility is in respect of personal data, collected, held and processed by CultureNL. 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 CultureNL complies with the Data Protection Laws.

(b) ensuring CultureNL and CultureNL staff are fully informed of their own legal responsibilities.

(c) Developing and managing CultureNL's Data Protection Policy, including development, implementation and enforcement of this policy and Data Protection procedures.

(d) reporting on CultureNL's compliance with the Data Protection Laws to the CultureNL board on a 6 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 CultureNL.

(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

The Chief Executive's responsibilities include:-

(a) ensuring that personal information 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 reporting immediately changes to the 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).

7.4 Service Managers

Service 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 dismissal is taken where an employee or worker has deliberately broken the terms of the Data Protection Laws or this policy or of any of CultureNL'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 give it out unlawfully;

(d) ensuring that all personal information held is accurate and up to date; and

(e) determining whether a Data Privacy Impact Assessment needs to be undertaken and, if so, putting in place appropriate arrangements to ensure that such a Data Protection Impact Assessment is undertaken and completed.

(f) identifying, documenting and informing the DPO of all categories of personal information held within their service.

(g) identifying, documenting and informing the DPO of all processing to which that personal information is put.

(h) identifying, documenting and informing the DPO how long personal information needs to be held within each Service.

(i) ensuring that necessary arrangements are in place in their service for the secure disposal of personal data.

(j) putting into place procedures for the secure destruction of any personal information immediately when CultureNL no longer needs to keep it.

(k) putting in place all arrangements and procedures as are 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.

(l) issuing instructions and putting into place 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 the said information is held.

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 CultureNL information policies, procedures and other guidance.

(c) report any observed or suspected breach of this data protection policy or related information procedure and guidance.

(d) ensure that 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.

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.

CultureNL must also conduct DPIAs in respect to high risk processing.

All Users 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 CultureNL'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. CultureNL currently follows the guidance provided by North Lanarkshire Council in Appendix 2 of its Data Protection Policy.

9. Data Protection Incidents/Breaches

Subject to certain exceptions, the GDPR requires data controllers to notify personal data breaches to the ICO and, in certain instances, the data subject.

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 of the North Lanarkshire Council Data Protection Policy).

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

CultureNL 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 CultureNL 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 Service Manager 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 Services and Third Parties

CultureNL must protect against processing personal information unlawfully. In most cases personal information can only be shared between 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 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 CultureNL 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 CultureNL 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.

CultureNL 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 code of practice in respect of data sharing arrangements between organisations has been issued by the ICO under the Data Protection Act 1998. The code explains how the 1998 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. The Code is still relevant to data sharing under the new Data Protection Laws but may be updated by the ICO.

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

14. Rights of Individuals

CultureNL, 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 CultureNL’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 DPO and will be subject to approval by board of CultureNL Ltd.

Appendix A: Glossary of Terms

Term	Description
The Act	Data Protection Act 2018
All Users	All parties who have access to CultureNL information including employees, elected members and third party contractors and any other individuals or organisations who access Council information.
CultureNL information	CultureNL 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.
Data Protection Laws	The GDPR and the Act
DPO	Data Protection Officer
DWP	Department of Work and Pensions
GDPR	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 CultureNL. CultureNL employees are excluded from this definition but it could include suppliers which handle personal data on behalf of CultureNL, for example where CultureNL outsources IT, payroll, paper waste disposal & mail shot / marketing services. CultureNL is the processor where it is providing services for another organisation who is determining the purpose and manner of processing, for example North Lanarkshire Council.