Leitrim County Council General Data Protection Policy

Document reference number	LCCDP01	**Revision number**	1.0
Document drafted by	K. Glancy	**Document reviewed by**	GDPR Working Group
Document approved by	LCC Management Team	**Document approved by**	23.11.2018
Next Review Date	01.12.2025	**Date of withdrawal of obsolete document**	

Amendment history			
Date	**Revision level**	**Details of amendment**	**Approval signature**

1. INTRODUCTION

1.1 Background to the General Data Protection Regulation

The General Data Protection Regulation 2016 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the "rights and freedoms" of natural persons (i.e. living individuals) and to ensure that Personal Data is processed in line with data protection principles and on a lawful basis (the "**GDPR**")

1.2 This Data Protection Policy sets out Leitrim County Council's commitment to protecting the rights and privacy of individuals and details how we will ensure compliance with the GDPR and Irish data protection legislation.

1.3 Interpretation

The defined terms used in this policy shall have the meanings given to them in Schedule 1 (Definitions) and in the GDPR.

2. POLICY STATEMENT AND SCOPE

2.1 The County Council recognises that the correct and lawful treatment of Personal Data will maintain confidence in the County Council and will provide for successful business operations. Protecting the confidentiality and integrity of Personal Data is a critical responsibility that we take seriously at all times.

2.2 Material scope (Article 2) – the GDPR applies to the processing of Personal Data wholly or partly by automated means (i.e. by computer) and to the processing other than by automated means of Personal Data (i.e. paper records) that form part of a filing system or are intended to form part of a filing system.

2.3 Territorial scope (Article 3) – the GDPR will apply to all Data Controllers that are established in the EU who process the Personal Data of Data Subjects, in the context of that establishment. It will also apply to controllers outside of the EU that process Personal Data in order to offer goods or services (irrespective of payment), or monitor the behaviour of Data Subjects in the EU.

2.4 The County Council, located at Leitrim County Council, Áras an Chontae, Carrick on Shannon, Co. Leitrim are committed to compliance with all relevant EU and Member State laws in respect of Personal Data, and the protection of the "rights and freedoms" of individuals whose information the County Council collects and processes in accordance with the GDPR.

2.5 Compliance with the GDPR is described by this Policy and the Related Policies, along with associated procedures.

2.6 The GDPR and this Policy apply to all of the County Council's Personal Data processing functions, including those performed on customers', clients', employees', suppliers' and others' Personal Data, and any other Personal Data the County Council processes from any source.

The DPO is responsible for ensuring the review of processing activities regularly in the light of any changes to the County Council's activities (as determined by changes to the data inventory register and the management review) and to any additional requirements identified by means of data protection impact assessments.

2.7 This Policy applies to all County Council Personnel. Any breach of the GDPR and/or the Related Policies will be dealt with under the County Council's disciplinary policy and may also be a criminal offence, in which case the matter will be reported as soon as possible to the appropriate authorities.

2.8 No third party may access Personal Data held by the County Council without having first entered into a data processing agreement and/or a Non-Disclosure Agreement, which imposes on the third party obligations no less onerous than those to which the County Council is committed, and which gives the County Council the right to audit compliance with the agreement.

2.9 Please contact the DPO with any questions about the operation of this Policy or the GDPR or if you have any concerns that this Policy is not being or has not been followed. In particular, you must always contact the DPO in the following circumstances:

2.9.1 if there has been a Personal Data Breach;

2.9.2 if you need any assistance dealing with any rights invoked by a Data Subject;

2.9.3 if you need help with any contracts or other areas in relation to sharing Personal Data with third parties (including our vendors);

2.9.4 if you are unsure of the lawful basis which you are relying on to process Personal Data;

2.9.5 if you need to rely on Consent and/or need to capture Explicit Consent;

2.9.6 if you need to draft privacy notices;

2.9.7 if you are unsure about the retention period for the Personal Data being processed;

2.9.8 if you are unsure about what security or other measures you need to implement to protect Personal Data;

2.9.9 if you are unsure on what basis to transfer Personal Data outside the EEA;

2.9.10 whenever you are engaging in a significant new, or change in, processing activity which is likely to require a DPIA (Data Privacy Impact Assessment) or plan to use Personal Data for purposes others than what it was collected for;

2.9.11 If you plan to undertake any activities involving Automated Processing including profiling or Automated Decision-Making; or

2.9.12 If you need help complying with applicable law when carrying out direct marketing activities.

3. RESPONSIBILITIES AND ROLES UNDER THE GENERAL DATA PROTECTION REGULATION

3.1 In the majority of instances, the County Council will act as Data Controller and sometimes as Data Controller and Data Processor in relation to Personal Data, however in some limited circumstances the County Council may act as Data Processor on behalf of another body/organisation.

3.2 The County Council is responsible for compliance with Data Protection Legislation and for being able to demonstrate such compliance.

3.3 Senior management and all those in managerial or supervisory roles throughout the County Council are responsible for developing and encouraging good information/ data handling practices within the County Council.

3.4 The DPO, a role specified in the GDPR, has the following tasks in relation to GDPR compliance:

3.4.1 to inform and advise the County Council and County Council Personnel of their obligations in relation to Data Protection Legislation where they are involved in processing of personal data;

3.4.2 to monitor compliance with the GDPR within the County Council with the assistance of nominated staff within each section of the County Council. This duty shall involve providing information, advice and recommendations to senior management in relation to achieving GDPR compliance;

3.4.3 to assist the County Council in carrying out DPIAs where necessary;

3.4.4 to co-operate with the Irish Data Protection Commission where required;

3.4.5 to act as the contact point for the Irish Data Protection Commission on issues relating to processing, including the prior consultation referred to in

Article 36 of the GDPR, and to consult, where necessary, with regard to any other matter;

3.4.6 to assist with and provide advice in relation to the preparation and implementation of policies and procedures put in place to demonstrate compliance with the Data Protection Legislation; and

3.4.7 to at all times in the performance of its tasks take a risk-based approach and prioritise its activities and focus its efforts on issues that present higher data protection risks.

3.5 Compliance with Data Protection Legislation is the responsibility of all County Council Personnelwho process Personal Data.

3.6 Training and awareness requirements for the County Council will be managed by HR Training in consultation with the Director of Services Corporate Services & Human Resources and the DPO.

3.7 County Council Personnel and the public are responsible for ensuring that any Personal Data about them and supplied by them to the County Council is accurate and up-to-date.

4. DATA PROTECTION PRINCIPLES

All processing of Personal Data must be conducted in accordance with the data protection principles as set out in Article 5 of the GDPR. The County Council's policies and procedures are designed to ensure compliance with the principles.

4.1 Personal Data must be processed lawfully, fairly and transparently.

Lawful – identify a lawful basis before you can process Personal Data. These are often referred to as the "conditions for processing", for example legislative basis.

Fairly – in order for processing to be fair, the Data Controller has to make certain information available to the Data Subjects as practicable. This applies whether the Personal Data was obtained directly from the Data Subjects or from other sources.

The GDPR has increased requirements about what information should be available to Data Subjects, which is covered in the 'Transparency' requirement.

Transparently –the GDPR includes rules on giving privacy information to Data Subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the Data Subject in an intelligible form using clear and plain language.

The County Council's Privacy Notice is recorded on the Council website at this address:
https://www.leitrim.ie/council/corporate-governance/data-protection/data-protection-policies/

The specific information that must be provided to the Data Subject must, as a minimum, include:

4.1.1 the identity and the contact details of the Data Controller and, if any, of the Data Controller's representative;

4.1.2 the contact details of the DPO;

4.1.3 the purposes of the processing for which the Personal Data are intended as well as the legal basis for the processing;

4.1.4 the period for which the Personal Data will be stored;

4.1.5 the existence of the rights to request access, rectification, erasure or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

4.1.6 the categories of Personal Data concerned;

4.1.7 the recipients or categories of recipients of the Personal Data, where applicable;

4.1.8 where applicable, that the Data Controller intends to transfer Personal Data to a recipient in a third country and the level of protection afforded to the data; and

4.1.9 any further information necessary to guarantee fair processing.

4.2 Personal Data can only be collected for specific, explicit and legitimate purposes.

4.2.1 Data obtained for specified purposes must not be used for other purposes, save where the GDPR provides for same.

4.3 Personal Data must be adequate, relevant and limited to what is necessary for processing.

4.3.1 The County Council must not collect information that is not strictly necessary for the purpose for which it is obtained.

4.3.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a fair processing statement or link to privacy statement.

4.3.3 The DPO will ensure that, on a regular basis all data collection methods are reviewed internally to ensure that collected data continues to be adequate, relevant and not excessive.

4.4 Personal Data must be accurate and kept up to date with every effort to erase or rectify without delay.

4.4.1 Personal Data that is stored by the Data Controller must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

4.4.2 The County Council has a Data Retention Policy which specifies that the County Council will follow the National Retention Policy for Local Authority Records other than where specific, separate retention periods are required.

4.4.3 The DPO, together with HR, will work together to ensure that all staff are trained in the importance of collecting accurate data and maintaining it.

4.4.4 It is also the responsibility of the Data Subject to ensure that data held by the County Council is accurate and up to date. Completion of a registration or application form by a Data Subject will include a statement that the data contained therein is accurate at the date of submission.

4.4.5 County Council Personnel should be required to notify the County Council of any changes in circumstance to enable personal records to be updated accordingly. Instructions for updating records are contained the Council's staff handbook. It is the responsibility of the County Council to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.6 The DPO will assist the County Council in ensuring that appropriate procedures and policies are in place to keep Personal Data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

4.4.7 On a regular basis, the DPO will arrange for a review of the retention dates of all the Personal Data processed by the County Council, by reference to the data inventory, in order to identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed or archived in line with the Data Retention Policy (in accordance with national guidelines) and following issue of a certificate of destruction by the County Council's authorised officer.

4.4.8 The DPO will have oversight for ensuring that requests for rectification from Data Subjects are responded to within one month. This can be extended to a further two months for complex requests. If the County Council decides not to comply with the request, the DPO will arrange for a response to the Data Subject to explain its reasoning and inform them of

their right to complain to the supervisory authority and seek judicial remedy.

4.4.9 The DPO will assist the County Council in making appropriate arrangements where third-party organisations may have been passed inaccurate or out-of-date Personal Data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned; and for passing any correction to the Personal Data to the third party where this is required.

4.5 Personal Data must be kept in a form such that the Data Subject can be identified only as long as is necessary for processing.

4.5.1 Personal Data will be retained in line with the Data Retention Policy and, once its retention date is passed, it must be securely destroyed or archived as described above.

4.5.2 The County Council's archivist or records manager (in consultation with the DPO where necessary) must specifically approve any data retention that exceeds the retention periods referred to in the Data Retention Policy, and must ensure that the justification is clearly identified and in line with the requirements of the Data Protection Legislation. This approval must be written.

4.6 Personal Data must be processed in a manner that ensures compliance with relevant security policies.

4.6.1 The DPO will ensure that a risk assessment is carried out taking into account all the circumstances of the County Council's controlling or processing operations. Each section shall be responsible for their own risk assessment with the oversight of the DPO.

4.6.2 In determining appropriateness, the County Council together with the DPO should also consider the extent of possible damage or loss that might be caused to individuals (e.g. staff or customers) if a security breach occurs, the effect of any security breach on the County Council itself, and any likely reputational damage including the possible loss of customer trust.

4.6.3 When assessing appropriate technical measures, the County Council together with the DPO will consider the following:

- Password protection;
- Automatic locking of idle terminals;
- Removal of access rights for USB and other memory media;
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;
- Encryption of devices that leave the County Council's premises such as laptops;

- Security of local and wide area networks;
- Privacy enhancing technologies such as pseudonymisation and anonymisation;
- Identifying appropriate international security standards relevant to the County Council; and
- Any other measure it considers appropriate.

4.6.4 When assessing appropriate organisational measures the County Council together with the DPO will consider the following:

- The appropriate training levels throughout the County Council;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- Identification of disciplinary action measures for data breaches;
- Monitoring of staff for compliance with relevant security standards;
- Physical access controls to electronic and paper based records;
- Adoption of a clear desk policy;
- Storing of paper based data in lockable fire-proof cabinets;
- Restricting the use of portable electronic devices outside of the workplace;
- Adopting clear rules about passwords;
- Making regular backups of Personal Data and storing the media off-site;
- The imposition of contractual obligations on the importing organisations to take appropriate security measures when transferring data outside the EEA; and
- Any other measure it considers appropriate.

These controls have been selected on the basis of identified risks to Personal Data, and the potential for damage or distress to individuals whose data is being processed.

4.7 The County Council must be able to demonstrate compliance with the GDPR's other principles (accountability).

4.7.1 The GDPR includes provisions that promote accountability and governance. These complement the GDPR's transparency requirements. The accountability principle in Article 5(2) requires the County Council to demonstrate that it complies with the principles and states explicitly that this is the County Council's responsibility.

4.7.2 The County Council will demonstrate compliance with the data protection principles by implementing data protection policies, adhering to codes of conduct, implementing technical and organisational measures, as well as adopting techniques such as data protection by design, DPIAs and breach notification procedures.

4.7.3 The County Council must implement appropriate technical and organisational measures in an effective manner, to ensure compliance with data protection principles. The County Council is responsible for, and must be able to demonstrate, compliance with the data protection principles.

4.7.4 The County Council must have adequate resources and controls in place to ensure and to document GDPR compliance including:

(a) appointing a suitably qualified DPO;

(b) implementing Privacy by Design when Processing Personal Data and completing DPIAs where Processing presents a high risk to rights and freedoms of Data Subjects;

(c) integrating data protection into internal documents including this Policy and Related Policies;

(d) regularly training County Council Personnel on the GDPR, this Policy and Related Policies and data protection matters including, for example, Data Subjects' rights, Consent, legal basis, DPIA and Personal Data Breaches. The County Council must maintain a record of training attendance by County Council Personnel; and

(e) regularly testing the privacy measures implemented and conducting periodic reviews and audits to assess compliance, including using results of testing to demonstrate compliance improvement effort.

4.7.5 <u>Record Keeping</u>

(a) The GDPR requires the County Council to keep full and accurate records of all its data processing activities.

(b) The County Council is required to keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining Consents

(c) These records should include, at a minimum, the name and contact details of the County Council and the DPO, clear descriptions of the Personal Data types, Data Subject types, processing activities, processing purposes, third-party recipients of the Personal Data, Personal Data storage locations, Personal Data transfers, the Personal Data's retention period and a description of the security measures in place. In order to create such records, data maps should be created which should include the detail set out above together with appropriate data flows.

4.7.6 Training and Audit

(a) The County Council is required to ensure all County Council Personnel have undergone adequate training to enable them to comply with data privacy laws. The County Council must also regularly test its systems and processes to assess compliance.

(b) The County Council is required to regularly review all the systems and processes under its control to ensure it complies with this Policy and check that adequate governance controls and resources are in place to ensure proper use and protection of Personal Data.

4.7.7 Privacy by Design and Data Protection Impact Assessment (DPIA)

The County Council is 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. The County Council 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.

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

(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 Personal Data; and

(d) large scale, systematic monitoring of a publicly accessible area.

4.7.9 A DPIA must include:

(a) a description of the processing, its purposes;

(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.

4.7.10 Automated Processing (including profiling) and Automated Decision-Making

Generally, Automated Decision Making is prohibited when a decision has a legal or similar significant effect on an individual unless:

(a) a Data Subject has Explicitly Consented;

(b) the Processing is authorised by law; or

(c) the Processing is necessary for the performance of or entering into a contract.

4.7.11 If certain types of Special Categories of Personal Data are being processed, then grounds (b) or (c) will not be allowed but such Special Categories of Personal Data can be processed where it is necessary (unless less intrusive means can be used) for substantial public interest like fraud prevention.

4.7.12 If a decision is to be based solely on Automated Processing (including profiling), then Data Subjects must be informed when you first communicate with them of their right to object. This right must be explicitly brought to their attention and presented clearly and separately from other information. Further, suitable measures must be put in place to safeguard the Data Subject's rights and freedoms and legitimate interests.

4.7.13 The County Council must also inform the Data Subject of the logic involved in the decision making or profiling, the significance and envisaged consequences and give the Data Subject the right to request human intervention, express their point of view or challenge the decision.

4.7.14 A DPIA must be carried out before any Automated Processing (including profiling) or Automated Decision Making activities are undertaken.

4.7.15 Sharing Personal Data

(a) Generally the County Council is not allowed to share Personal Data with third parties unless certain safeguards and contractual arrangements have been put in place.

(b) Personal Data may only be shared with another employee, agent or representative of the County Council if the recipient has a job-

related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

4.7.16 Personal Data held by the County Council may only be shared with third parties, such as our service providers 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 Statement 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 fully executed written contract that contains GDPR approved third party clauses has been obtained.

4.8 Submissions by Elected Representatives to the Council

4.8.1 Elected Representatives are acting as Data Controllers when making representations on behalf of their constituents. When the Elected Representative submits a representation to the Council, relating to a constituent's personal data;

(a) only representations received from Elected Representatives in writing (either by letter or email), will be processed by the Council.

(b) the Council and its employees will process the representation received, based on the requirement that the Elected Representative has a legal basis for processing this data and the constituent has agreed to this transfer.

(c) in respect of all representations received by email, the Council's staff will respond to all such representations using only the email address provided to the Elected Representative by the Council.

(d) if Council staff consider that the relevant person is unaware of the submission on their behalf, then the Elected Representative must demonstrate that this person has consented to this data transfer.

4.9 Responses to the Elected Representatives from the Council

4.9.1 When an Elected Representative makes a representation;

(a) Representations not requiring the release of personal data:

If the representation is an enquiry about a service and no personal data (other than that originally contained in the request) needs to be used in the reply, the reply will issue directly to the Elected Representative. This therefore means that where personal data is not to be issued in the reply, that the request and reply may be made in any form (i.e. written, verbal, etc.).

(b) Representations requiring the release of personal data:

If the representation is an enquiry that requests personal data to be released (other than the personal data originally contained in the request) and if the Elected Representative submits the completed 'Verification Form', the Council staff will respond directly to the Elected Representative. All responses are to be sent by email to the email address provided to the Elected Representative by the Council (i.e. xxxxxx@leitrimcoco.ie).

A blank 'Verification Form' is included in Appendix 1. A 'Verification Form' can be submitted for individual requests or a 'Verification form' can be submitted for multiple requests relating to the same process and the same data subject.

If the representation is an enquiry that requests personal data to be released (where the request relates to data that is extra to what was in the representation received) and the representation does not include the 'Verification Form', the reply will issue to the Data Subject or the person legitimately acting on behalf of the Data Subject. The content of the response will refer to the representation being made by the Elected Representative who made the request. An email notification will also be sent to the Elected Representative to state that a response has issued in relation to the representation.

Each Council is to nominate staff in each department at an appropriate level to review each response which contains personal data to be released (other than the personal data originally contained in the request). A checklist is included in Appendix 2 to be used by the nominated staff member to assist with this review.

5. CONSENT

5.1 In general, the County Council does not rely on Consent as a legal basis for processing Personal Data however there are limited circumstances in which we will rely on Consent.

5.2 The County Council understands 'Consent' to mean that it has been explicitly and freely given, and a specific, informed and unambiguous indication of the Data Subject's wishes that, by statement or by a clear affirmative action, signifies agreement to the processing of Personal Data relating to him or her. The Data Subject can withdraw their Consent at any time.

5.3 The County Council understands 'Consent' to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, while in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

5.4 There must be some active communication between the parties to demonstrate active Consent. Consent cannot be inferred from non-response to a communication. The Controller must be able to demonstrate that Consent was obtained for the processing operation.

5.5 For Special Categories of Personal Data, explicit written Consent of Data Subjects must be obtained unless an alternative legitimate basis for processing exists.

5.6 Where the County Council provides online services to children, parental or custodial authorisation must be obtained. This requirement applies to children under the age of 16.

6. DATA SUBJECTS' RIGHTS

6.1 Data Subjects have the following rights regarding data processing, and the data that is recorded about them:

6.1.1 To make subject access requests regarding the nature of information held and to whom it has been disclosed.

6.1.2 To prevent processing likely to cause damage or distress.

6.1.3 To prevent processing for purposes of direct marketing.

6.1.4 To be informed about the mechanics of automated decision-taking process that will significantly affect them.

6.1.5 To not have significant decisions that will affect them taken solely by automated process.

6.1.6 To sue for compensation if they suffer damage by any contravention of the GDPR.

6.1.7 To take action to rectify, block, erase, including the right to be forgotten, or destroy inaccurate data.

6.1.8 To request the supervisory authority to assess whether any provision of the GDPR has been contravened.

6.1.9 To have Personal Data provided to them in a structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.

6.1.10 To object to any automated profiling that is occurring without Consent.

6.1.11 To withdraw Consent to processing at any time where Consent is used as a legal basis for processing.

6.1.12 To restrict processing in specific circumstances.

6.1.13 To challenge processing which has been justified on the basis of legitimate interests or in the public interest. The County Council cannot rely on legitimate interests as a legal basis for processing.

6.1.14 To request a copy of an agreement under which Personal Data is transferred outside of the EEA.

6.1.15 To be notified of a Personal Data Breach which is likely to result in high risk to their rights and freedoms.

6.2 The County Council ensures that Data Subjects may exercise these rights:

6.2.1 Data Subjects may make data access requests as described in Subject Access Request Procedure; this procedure also describes how the County Council will ensure that its response to the data access request complies with the requirements of the GDPR.

6.2.2 Data Subjects have the right to complain to the County Council in relation to the processing of their Personal Data, the handling of a request from a Data Subject and appeals from a Data Subject on how complaints have been handled.

7. SECURITY OF DATA AND PERSONAL DATA BREACHES

7.1 All County Council Personnel are responsible for ensuring that any Personal Data that the County Council holds and for which they are responsible, is kept securely and is not under any conditions disclosed to any third party unless that third party has been specifically authorised by the County Council to receive that information and has entered into a data processing agreement.

7.2 All Personal Data should be accessible only to those who need to use it, and access may only be granted in line with the User Access Control Policy All Personal Data should be treated with the highest security and must be kept:

- in a lockable room with controlled access; and/or

- in a locked drawer or filing cabinet; and/or
- if computerised, password protected in line with corporate requirements in the ICT User Access Policy; and/or
- stored on (removable) computer media which are encrypted in line with ICT Information Security Policy.

7.3 Care must be taken to ensure that PC screens and terminals are not visible except to authorised County Council Personnel. All County Council Personnel are required to confirm that have received and read the ICT Information Security Policy. before they are given access to organisational information of any sort, which details rules on screen time-outs.

7.4 Manual records may not be left where they can be accessed by unauthorised personnel and may not be removed from business premises without explicit authorisation. As soon as manual records are no longer required for day-to-day client support, they must be removed from secure archiving in line with LCC data Retention Policy.

7.5 Personal Data may only be deleted or disposed of in line with the Data Retention Policy. Manual records that have reached their retention date are to be shredded and disposed of as 'confidential waste' following issue of a certificate of destruction from the Archivist of the County Council. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Data Retention Policy.

7.6 Processing of Personal Data 'off-site' presents a potentially greater risk of loss, theft or damage to Personal Data. Staff must be specifically authorised to process data off-site.

7.7 The GDPR requires Data Controllers to notify any Personal Data Breach to the applicable regulator and, in certain instances, the Data Subject.

7.8 The County Council has put in place procedures to deal with any suspected Personal Data Breach and will notify Data Subjects or any applicable regulator where the County Council is legally required to do so.

7.9 If you know or suspect that a Personal Data Breach has occurred, do not attempt to investigate the matter yourself. Immediately contact the person or team designated as the key point of contact for Personal Data Breaches and the DPO. You should preserve all evidence relating to the potential Personal Data Breach.

8. DISCLOSURE OF DATA

8.1 The County Council must ensure that Personal Data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, relevant law enforcement bodies. All County

Council Personnel should exercise caution when asked to disclose Personal Data held on another individual to a third party. It is important to bear in mind whether or not disclosure of the information is relevant to, and necessary for, the conduct of the County Council's business.

8.2 There are circumstances where the County Council will be required by law to make certain information available to other government bodies or relevant law enforcement bodies which may include Personal Data.

8.3 All requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

9. RETENTION AND DISPOSAL OF DATA

9.1 The County Council shall not keep Personal Data in a form that permits identification of Data Subjects for longer a period than is necessary, in relation to the purpose(s) for which the data was originally collected.

9.2 The County Council may store data for longer periods if the Personal Data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the implementation of appropriate technical and organisational measures to safeguard the rights and freedoms of the Data Subject.

9.3 The retention period for each category of Personal Data is set out in the National Retention Policy for Local Authority Records and, where applicable, in the County Council's Data Retention Policy along with the criteria used to determine this period including any statutory obligations the County Council has to retain the data.

9.4 The County Council's data retention and data disposal policies are set out in the County Council's Data Retention Policy and will apply in all cases.

9.5 Personal Data must be disposed of securely in accordance with the sixth principle of the GDPR – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of Data Subjects. Any disposal of data will be done in accordance with the National Retention Policy for Local Authority Records.

10. INFORMATION ASSET REGISTER/DATA INVENTORY

10.1 Leitrim County Council will establish a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR

compliance project. The County Council's data inventory and data flow determines:

- business processes that use Personal Data;
- source of Personal Data;
- volume of Data Subjects;
- description of each item of Personal Data;
- processing activity;
- maintains the inventory of data categories of Personal Data processed;
- documents the purpose(s) for which each category of Personal Data is used;
- recipients, and potential recipients, of the Personal Data;
- the role of the County Council throughout the data flow;
- key systems and repositories; and
- all retention and disposal requirements.

10.2 The County Council assesses risks associated with the processing of particular types of Personal Data.

10.2.1 The County Council assesses the level of risk to individuals associated with the processing of their Personal Data. DPIAs will be carried out in relation to the processing of Personal Data by the County Council, and in relation to processing undertaken by other organisations on behalf of the County Council.

10.2.2 The County Council shall manage any risks identified by the risk assessment in order to reduce the likelihood of a non-conformance with this Policy.

10.2.3 Where a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing is likely to result in a high risk to the rights and freedoms of natural persons, the County Council shall, prior to the processing, carry out a DPIA of the impact of the envisaged processing operations on the protection of Personal Data. A single DPIA may address a set of similar processing operations that present similar high risks.

10.2.4 Where, as a result of a DPIA it is clear that the County Council is about to commence processing of Personal Data that could cause damage and/or distress to the Data Subjects, the decision as to whether or not the County Council may proceed must be escalated for review to the DPO.

10.2.5 The DPO shall, if there are significant concerns, either as to the potential damage or distress, or the quantity of data concerned, escalate the matter to the supervisory authority.

10.2.6 Appropriate controls will be applied to reduce the level of risk associated with processing individual data to an acceptable level and the requirements of the GDPR.

11. DOCUMENT OWNER AND APPROVAL

11.1 The DPO is the owner of this document and is responsible for ensuring that this Policy document is reviewed in line with the review requirements stated above.

11.2 A current version of this document is available to all members of staff on the Council Intranet.

11.3 This Policy was approved by the County Council on 22nd November 2018 and is issued on a version-controlled basis under the signature of the Chief Executive

11.4 This Policy does not override any applicable national data privacy laws and regulations in countries where Leitrim County Council operates.

SCHEDULE 1
DEFINITIONS

"Automated Decision-Making (ADM)" **–** when a decision is made which is based solely on Automated Processing (including Profiling) which produces legal effects or significantly affects an individual. The GDPR prohibits Automated Decision-Making (unless certain conditions are met) but not Automated Processing.

"Automated Processing**"** **–**any form of automated processing of Personal Data consisting of the use of Personal Data to evaluate certain personal aspects relating to an individual, in particular to analyse or predict aspects concerning that individual's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Profiling is an example of Automated Processing.

"Child"**–** the GDPR defines a child for the purposes of receiving information services as anyone under the age of 16 years old, although this may be lowered to 13 by Member State law. Where a Data Controller relies on Consent as the legal basis for processing under Article 6(1)(a) of the GDPR, the processing of Personal Data of a child in relation to information society services is only lawful if authorised by the holder of parental responsibility over the child. The Data Controller shall make reasonable efforts to verify in such cases that Consent is given or authorised by the holder of parental responsibility over the child.

"Consent"**–** agreement which must be freely given, specific, informed and be an unambiguous indication of the Data Subject's wishes by which they, by a statement or by a clear positive action, signify agreement to the Processing of Personal Data relating to them.

"Data Controller" – the natural or legal person, public authority, agency or other body which, alone, or jointly with others, determines the purposes and means of the Processing of Personal Data where the purposes and means of such Processing are determined by European Union ("**EU**") or Member State law, the Data Controller, or the specific criteria for its nomination is provided for by EU or Member State law.

"Data Processor" – the natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Data Controller.

"Data Privacy Impact Assessment (DPIA)" – tools and assessments used to identify and reduce risks of a data processing activity. DPIA can be carried out as part of Privacy by Design and should be conducted for all major system or business change programs involving the Processing of Personal Data.

"Data Protection Officer (DPO)" – the person required to be appointed in specific circumstances under the GDPR. Where a mandatory DPO has not been appointed, this term means a data protection manager or other voluntary appointment of a

DPO or refers to the County Council's data privacy team with responsibility for data protections compliance.

"Establishment" **–** the main establishment of the Data Controller in the EU will be the place in which the Data Controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a Data Processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the Data Controller operates to act on behalf of the Data Controller and deal with supervisory authorities.

"Explicit Consent" **–** Consent which requires a very clear and specific statement (that is, not just action).

"Filing System"– any structured set of Personal Data which is accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

"Member State" – any member state of the European Union.

"County Council"- Leitrim County Council.

"County Council Personnel" **–** all employees, workers, directors, elected members and others.

"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.

"Personal Data Breach" **–** 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. There is an obligation on the Data Controller to report Personal Data breaches to the supervisory authority and where the breach is likely to adversely affect the Personal Data or privacy of the Data Subject.

"Policies" or "Related Policies"-This General Data Protection Policy, County Council policies, operating procedures or processes related to this Policy and designed to protect Personal Data, a list of which is contained at Schedule 2, as may be updated by the County Council from time to time.

"Privacy by Design" implementing appropriate technical and organisational measures in an effective manner to ensure compliance with the GDPR.

"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.

"Profiling" **–** is any form of Automated Processing of Personal Data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the Data Subject to object to Profiling and a right to be informed about the existence of Profiling, of measures based on Profiling and the envisaged effects of Profiling on the individual.

"Special Categories of Personal Data" – Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

"Third party" – a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorised to process Personal Data.

SCHEDULE 2
RELATED POLICIES

1. Data Retention Policy & Procedures
2. Data Breach Policy & Procedure
3. Data Access Request Policy & Procedure
4. Website Data Privacy Statement
5. CCTV Policy

Appendix 1 – Verification Form

Form for an Elected Representative to Receive Personal Data

The following describes the enquiry that the Elected Representative will make on my behalf and I acknowledge that the Elected Representative may receive personal data, in accordance with the provisions of Section 40 of the Data Protection Act 2018, for the purpose of a response to this enquiry:

Details of my enquiry:

_____

_____

_____

_____

_____

_____

Signature (of person making request): _____ *(not the Elected Representative)*

Date: _____

For verification purposes

Name of Person subject of the request (data subject):

_____

Address of Person subject of the request (data subject):

_____

_____

If the person making the request is not the subject

(Please provide consent of the data subject or statement as to why consent cannot be provided)

Please print name of person making the request: _____

State relationship to the data subject: _____

ELECTED REPRESENTATIVE DECLARATION

When I receive personal data from ---------- County Council, I confirm that I will take suitable and specific measures to safeguard the fundamental rights and freedoms of the person this representation relates to and process the information in accordance with Section 40 of the Data Protection Act 2018.

Name: Cllr./Deputy/Senator_____

Signature: _____

Appendix 2 – Checklist

1.0 Receiving the representation:

a) Is the representation merely an enquiry about a service (that does not require the issuing of personal data, other than that originally contained in the request)?

If YES – Proceed as per 3 (a) on this checklist.

b) Will the representation require the issue of new personal data in the reply?

If YES – The employee drafting the reply must have regard to Item 2 below and the reply must issue in line with 3 (b) or (c) on this checklist.

2.0 Processing the representation:

a) The person preparing the reply must make every effort to ensure that the reply
   i. Only contains personal data where absolutely necessary to respond to the enquiry.
   ii. Where personal data is necessary that it is limited to the minimum amount required to reply.

3.0 Issuing the reply:

a) If the representation is merely an enquiry about a service the reply can issue directly to the Elected Representative by any medium (i.e. written, verbal, etc.)

b) If the representation requires the issue of new personal data and the Elected Representative submits the completed Verification Form, the Council will reply to the Elected Representative.

i. Replies must always be by email and to the official email address provided to the Elected Representative by the Council (e.g. xxxxx@leitrimcoco.ie)

c) If the Elected Representative has not provided a completed Verification Form, do the following:
   i. Issue the reply to the Data Subject or the person legitimately acting on behalf of the Data Subject.
   ii. Ensure the reply refers to the representation being made by the Elected Representative.
   iii. Issue an email notification to the Elected Representative to state that a response has issued in relation to the representation.

d) All replies involving disclosure of personal data must be signed by the nominated staff member approved for that purpose.