GENERAL DATA PROTECTION POLICY
LIMERICK CITY AND COUNTY COUNCIL

COMHAIRLE
CATHRACH & CONTAE
Luimnigh
Limerick
CITY & COUNTY
COUNCIL

Table of Contents

1 Introduction

1.1 Background to the General Data Protection Regulation and the Law Enforcement Directive.

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**")

The Data Protection Act 2018 amended the Data Protection Act 1988 and, inter alia, enacted the Law Enforcement Directive (LED) which applies to; the processing of personal data for the purpose of the prevention, investigation, detection or prosecution of criminal offences including the safeguarding against, and the prevention of, treats to public security or; the execution of criminal penalties. From a data processing perspective, the enforcement functions of the Council will be processed primarily in accordance with the requirements of the LED, as enacted by Part 5 the Data Protection Act 2018.

1.2 This Data Protection Policy sets out Limerick City and 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. Specific reference will be made to the application of the LED, where applicable.

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 Council recognises that the correct and lawful treatment of Personal Data will maintain confidence in the 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 Limerick City and County Council, located at Merchants Quay 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 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 connected procedures.

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

2.7 This Policy applies to all Council Personnel. Any breach of the GDPR and/or the Related Policies may be dealt with under the City and 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 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:

2.8.1 if there has been a Personal Data Breach;

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

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

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

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

2.8.6 if you need to draft privacy notices;

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

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

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

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

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

2.8.12 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 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 Council may act as Data Processor on behalf of another body/organisation.

3.2 The 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 Council are responsible for developing and encouraging good information/data handling practices within the 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 Council and 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 City and County Council with the assistance of nominated staff within each section of the 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 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 Council Personnel who process Personal Data.

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

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

3.8 Information and Data Protection Champions in each Department will act as the first point of contact for issues relating to data protection including, data subject access requests, third party access requests and breaches. Acting in conjunction with their

Department Head, the Information and Data Protection Champions will report regularly on the status of a set of data protection topics to the DPO/Data Protection Monitoring Committee.

3.9 A Data Protection Monitoring Committee, comprised of Senior Staff from a range of Departments across the Council, in conjunction with the DPO will monitor compliance with data protection requirements throughout the Council and review quarterly updates from each Department in relation to same. The Committee will report key findings and recommendations to the Management Team.

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 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 Council's Privacy Statement is recorded on its website.

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.

4.1.10 The Council will publish Privacy Statements in respect of each service on the Service Catalogue that processes personal data and as appropriate. Any Privacy Statements that relate only to the personal data of Council Employees will be published on the Council's Intranet. The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that Privacy Statements for their Department are in place, kept accurate, up to date and in accordance with this policy. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

4.1.11 As Privacy Statements are based on services in the Council's Service Catalogue that process personal data, any changes agreed to the Service Catalogue by the Business Improvement Unit must be communicated to the relevant Department's Information and Data Protection Champion, the DPO and Records Management.

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.

4.2.2 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that data obtained for the purposes as set out in that Department's Privacy Statements is not used for other non-compatible purposes. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement. Any issues regarding the compatibility of further processing should be raised with the DPO.

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

4.3.1 The 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 link to privacy statement.

4.3.3 The Council's email system must not be used as a repository for personal data relating to our Customers. Any email relating to a service should be saved to the appropriate location in Sharepoint and/or printed and placed on the hardcopy file, where hardcopy files are required. The email should then be deleted from the email system.

4.3.4 The Information and Data Protection Champion, in conjunction with the Department Head, shall arrange, on a regular basis, for all data collection methods to be reviewed to ensure that collected data continues to be adequate, relevant and not excessive. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

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

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

4.4.4 Council Personnel should be required to notify the Council of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of the Council to ensure that any notification regarding change of circumstances is recorded and acted upon.

4.4.5 The DPO will assist the 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.

4.4.6 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 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.

4.4.7 The DPO will assist the 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.

4.4.8 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure 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. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

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 The 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.

4.5.2 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 Council's Data Retention Policy along with the criteria used to determine this period including any statutory obligations the Council has to retain the data.

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

4.5.4 The 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.

4.5.5 Where Personal Data is retained beyond the processing date, consideration will be given, where possible, to ***minimised/encrypted/pseudonymised*** the data in order to protect the identity of the Data Subject in the event of a data breach.

4.5.6 The 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.

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

4.5.8 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. Hard drives of redundant PCs are to be removed and immediately destroyed as required by the Records Retention Policy.

4.5.9 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.

4.5.10 The Information and Data Protection Champion, in conjunction with the Department Head shall, on a regular basis, arrange for a review of the retention dates of all the Personal Data processed by their Department, 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 and following issue of a certificate of destruction by the City and County Council's Archivist. Reports shall be provided annually by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

4.6 Personal Data must be processed in a manner that ensures the appropriate security.

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

4.6.2 In determining appropriateness of security, the 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 Council itself, and any likely reputational damage including the possible loss of customer trust.

4.6.3 When assessing appropriate technical measures, the 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; (This is currently under investigation with a view to implementation, as appropriate, in 2019)
- Virus checking software and firewalls;
- Role-based access rights including those assigned to temporary staff;

- Encryption of devices that leave the 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 Council; and
- Any other measure it considers appropriate.

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

- The appropriate training levels throughout the Council;
- Measures that consider the reliability of employees (such as references etc.);
- The inclusion of data protection in employment contracts;
- 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;
- Restricting the use of employee's own personal devices being used in the workplace;
- Adopting clear rules about passwords;
- Making regular backups of Personal Data and storing the media off-site; and
- 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.

4.6.5 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that a risk assessment is carried out taking into account all the circumstances of the Council's controlling or processing operations. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement. Reports shall be in the form of an agreed template that references the above technical and organisational measures and will provide for testing of the privacy measures implemented and using results of testing to demonstrate compliance improvement effort.

4.7 The 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 Council to demonstrate that it complies with the principles and states explicitly that this is the Council's responsibility.

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

4.7.4 The 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 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 Council must maintain a record of training attendance by 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 Record Keeping

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

(a) Data Inventory - The Council maintains a data inventory and data flow process as part of its approach to address risks and opportunities throughout its GDPR compliance project. The 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;
- any data transfers; and
- all retention and disposal requirements.

(b) **Record of Processing Activities (ROPA)** - Should include, at a minimum, the name and contact details of the 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.

The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that the Record of Processing Activities (ROPA) and Data Inventory reflect the processing activities for that Department, are accurate and up to date. The ROPA should be reviewed regularly in the light of any changes to the Department's activities (as determined by changes to the Service Catalogue or data inventory register) and to any additional requirements identified by means of data protection impact assessments. This register needs to be available on the supervisory authority's request.

As the ROPA is based on services in the Council's Service Catalogue that process personal data, any changes agreed to the Service Catalogue by the Business Improvement Unit must be communicated to the relevant Department's Information and Data Protection Champion, the DPO and Records Management.

Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirements.

(c) **Data Logging for Automated Processing Systems under the Law Enforcement Directive**. - A log of the following must be maintained in respect any such automated processing and be available for inspection to the Data Protection Commission:

- The collection of personal data for the purpose of such processing and the alteration of any data;
- The consultation of the personal data by any person;
- The disclosure of the personal data, including the transfer of the data, to any other person;
- The combination of the personal data with other data;
- The erasure of the personal data , or some of the data.

It should be noted that for automated processing systems established before 6th May 2016 the Act provides compliance dates of 2023 and 2026, subject to conditions.

The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that the appropriate logs are maintained in relation to automated processing under the LED.
Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirements.

4.7.6 Training and Audit

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

(b) The Council is required to undergo all mandatory data privacy related training and ensure all teams undergo similar mandatory training .

(c) The 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

The 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 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.

The Information and Data Protection Champion, in conjunction with the Department Head, must assess what Privacy by Design measures can be implemented on all programs/systems/processes to implement data protection principles in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of the GDPR and protect the rights of data subjects.
Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirements.

4.7.8 Data Protection Impact Assessment (DPIA)

(a) The 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 Council, and in relation to processing undertaken by other organisations on behalf of the Council.

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

(c) 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 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.

(d) Where the system under review includes the use of information communication technologies, the ICT Department and/or Digital Services Department will, as part of the DPIA, provide an assessment of the data security of the system to include risks, existing controls and any additional controls required.

(e) Where, as a result of a DPIA it is clear that the 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 Council may proceed must be escalated for review to the DPO.

(f) 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.

(g) Appropriate controls will be selected and applied to reduce the level of risk associated with processing individual data to an acceptable level in compliance with the requirements of the GDPR.

(h) The Council must conduct DPIAs in respect to high risk processing.

- use of new technologies (programs, systems or processes), or changing technologies (programs, systems or processes);
- Automated Processing including profiling and Automated Decision Making;
- large scale processing of Special Categories of Personal Data; and
- large scale, systematic monitoring of a publicly accessible area.

(i) A DPIA must include:

- a description of the processing, its purposes;
- an assessment of the necessity and proportionality of the processing in relation to its purpose;
- an assessment of the risk to individuals; and
- the risk mitigation measures in place and demonstration of compliance.

The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that DPIAs are carried out in accordance with this policy and any guidance issued by the Data Protection Commission.
Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirements.

4.7.9 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.

4.7.10 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.

4.7.11 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.

4.7.12 The 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.

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

4.7.14 Sharing Personal Data

(a) Generally the 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 Council if the recipient has a job-related need to know the information and the transfer complies with any applicable cross-border transfer restrictions.

4.7.15 Personal Data held by the 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.

5 Data Processing Agreements

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

5.2 The Council has a template Data Processing Agreement in place which provides the basis for the agreement between the Council as Data Controller and the third party, as Data Processor. The agreement requires the Data Processor to enter details of the security measures in place to protect the Council's data and also any sub-processors used by the third party. In general, a Data Processing Agreement is required with any service provider with whom a Department shares its customers' personal data.

5.3 It is the duty of each Department to ensure that it is satisfied with the data protection controls listed by the third party. Any queries in this regard should be raised with the ICT Department or the DPO, as appropriate. Any unresolved issues in relation to Data Processing Agreements will be brought to the Data Protection Monitoring Committee for consideration.

5.4 Copies of signed Data Protection Agreements must be forwarded to the DPO to facilitate logging of same.

5.5 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that Data Processing Agreements are in place with all third party service providers with whom that Department shares personal data. Using Agresso FMS, regular reviews of the third party service providers paid by the Department should be made to assist in this regard. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

6 Consent

6.1 In general, the 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.

6.2 The 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.

6.3 The 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.

6.4 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.

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

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

6.7 The Council is required to keep and maintain accurate corporate records reflecting our processing including records of Data Subjects' Consents and procedures for obtaining Consents.

6.8 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that records of Data Subjects' Consents and procedures for obtaining Consents are kept in the limited circumstances where Consent is relied upon as the Lawful Basis for processing.

7 Data Subjects' Rights

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

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

7.1.2 To prevent processing likely to cause damage or distress.

7.1.3 To prevent processing for purposes of direct marketing.

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

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

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

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

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

7.1.9 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.

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

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

7.1.12 To restrict processing in specific circumstances.

7.1.13 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.

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

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

7.2 The Council ensures that Data Subjects may exercise these rights:

7.2.1 Data Subjects may make data access requests as described in the Council's Response Policies and Procedures for Data Subject; this procedure also describes how the Council will ensure that its response to the data access request complies with the requirements of the GDPR.

7.2.2 Data Subjects may seek an internal review of how their request to exercise their rights under the GDPR and the Data Protection Act 2018 were dealt with by the Council. This internal review will be carried out by the Senior Executive Officer, Corporate Services.

8 Security of Data

8.1 All Council Personnel are responsible for ensuring that any Personal Data that the 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 Council to receive that information and has entered into a data processing agreement.

8.2 All Personal Data should be accessible only to those who need to use it. 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;

8.3 Council personal computers have been configured to ensure that data can only be copied from these devices to encrypted removable storage media, issued by the ICT Department with the approval of an employee's Supervisory Officer

8.4 Care must be taken to ensure that PC screens and terminals are not visible except to authorised Council Personnel. All Council Personnel are required to enter into an ICT Usage Policy before they are given access to organisational information of any sort.

8.5 Manual records may not be left where they can be accessed by unauthorised personnel. As soon as manual records are no longer required for day-to-day client support, they must be moved to secure archiving in line with our Data Retention Policy.

8.6 Manual records containing personal data should only be removed from our business premises where absolutely necessary. Any staff removing such files should, in conjunction with their line manager, maintain a record of what is being removed. This is to facilitate the Council in responding appropriately to any subsequent loss of the records. The following points should be adhered to in relation to laptops, portable electronic devices or files containing personal data;

8.6.1 Staff must not leave laptops, portable electronic devices or files containing personal information unattended in cars.

8.6.2 In cases where staff remove files or records from offices to attend meetings, site visits, etc the records should always be contained in a suitable brief case or bag to avoid inappropriate viewing and also to secure the records.

8.6.3 All files and portable equipment must be stored securely. If files containing personal data must be transported in a car, they should be locked securely in the boot for the minimum period necessary.

8.6.4 Staff should not take council records home, however, in exceptional cases where this can not be avoided, the records must be stored securely. Council records should not be left in a car overnight but stored securely indoors.

8.6.5 Staff should not use email or electronic storage media to tranfer records containing personal data for work on their private home PC or other non Council device. Any such PC or private email account may not have the appropriate level of security.

8.6.6 In general, remote working should be carried out using a Council managed device (that is a PC, laptop, tablet or other mobile device supplied by LCCC) and you are authorised for remote access.

8.6.7 The use of your private home computer to access Council files and systems using Citrix software, authorised and installed by the Council, does not pose a threat to those files or systems.

8.6.8 Take precautions to safeguard the security of any computer equipment on which you do LCCC business, and keep your passwords secure and secret.

8.6.9 Position yourself so that your work cannot be overlooked by others, not authorised to see the information.

8.6.10 Lock laptop screens or shut them down completely when they are not in use.

8.6.11 Never allow an unauthorised individual access to your device or LCCC information.

8.6.12 Avoid work conversations near Smart Speakers; - If you have a Digital Home Assistant device/Smart Speaker such as Alexa, Siri or Google Home, be aware that these devices are always 'listening' to conversations and potentially storing the recording. Bear this in mind if conducting work-related telephone calls or video conference calls, e.g. about customer confidential issues. It is recommended that you unplug the device or move to a different location in your home for the duration of the conversation.

8.6.13 Any loss of laptops or portable electronic devices should be reported immediately to the ICT Department and the Data Protection Officer.

8.6.14 Any loss of files containing personal information should be reported immediately to your line manager and the Data Protection Officer.

8.6.15 The Information and Data Protection Champion, in conjunction with the Department Head, shall ensure that procedures are in place to log the removal offsite and return of manual files containing personal data. Quarterly reports shall be provided by the Information and Data Protection Champion in each Department to the DPO outlining the position in relation to this requirement.

9 Personal Data Breaches

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

9.2 The Council has a Data Breach Policy that puts in place procedures to deal with any suspected Personal Data Breach. The Council will notify Data Subjects or any applicable regulator where the Council is legally required to do so.

9.3 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, the DPO or the information technology department and follow the Incident Response Policy/Breach Notification Policy. You should preserve all evidence relating to the potential Personal Data Breach.

9.4 The Information and Data Protection Champion, in conjunction with the Department Head will give quarterly updates to the DPO on the implementation of the Data Breach Policy in their Department

10 Disclosure of Data

10.1 The 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 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 Council's business.

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

10.3 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.

11 Data Transfers

11.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the Data Subjects".
The transfer of Personal Data outside of the EEA is prohibited unless one or more of the specified safeguards, or exceptions, apply:

11.1.1 An adequacy decision

The European Commission can and does assess third countries, a territory and/or specific sectors within third countries to assess whether there is an appropriate level of protection for the rights and freedoms of natural persons. In these instances no authorisation is required.

Countries that are members of the European Economic Area (EEA) but not of the EU are accepted as having met the conditions for an adequacy decision.
A list of countries that currently satisfy the adequacy requirements of the Commission are published in the *Official Journal of the European Union.* *http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm*

11.1.2 Privacy Shield

If the Council wishes to transfer Personal Data from the EU to an organisation in the United States it should check that the organisation is signed up with the Privacy Shield framework at the U.S. Department of Commerce. The obligation applying to companies under the Privacy Shield are contained in the "Privacy Principles". The US DOC is responsible for managing and administering the Privacy Shield and ensuring that companies live up to their commitments. In order to be able to certify, companies must have a privacy policy in line with the Privacy Principles e.g. use, store and further transfer the Personal Data according to a strong set of data protection rules and safeguards. The protection given to the Personal Data applies regardless of whether the Personal Data is related to an EU resident or not. Organisations must renew their "membership" to the Privacy Shield on an annual basis. If they do not, they can no longer receive and use Personal Data from the EU under that framework.

11.1.3 Assessment of adequacy by the Data Controller

In making an assessment of adequacy, the exporting controller should take account of the following factors:

- the nature of the information being transferred;
- the country or territory of the origin, and final destination, of the information;
- how the information will be used and for how long;
- the laws and practices of the country of the transferee, including relevant codes of practice and international obligations; and

- the security measures that are to be taken as regards the data in the overseas location.

11.1.4 Model contractual clauses

The Council may adopt approved model contractual clauses for the transfer of data outside of the EEA. If the County Council adopts the *[model contract clauses approved by the relevant supervisory authority]* there is an automatic recognition of adequacy.

11.1.5 Exceptions

In the absence of an adequacy decision, Privacy Shield membership, binding corporate rules and/or model contract clauses, a transfer of Personal Data to a third country or international organisation shall only take place on one of the following conditions:

- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims; and/or
- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving Consent.

12 Document Owner and Approval

12.1 The DPO is the owner of this document and is responsible for ensuring that this Policy document is reviewed annually in conjunction with the Data Protection Monitoring Committee and in line with the review requirements stated above.

12.2 The Council reserves the right to change this Policy at any time without notice to Council Personnel so please check back regularly to obtain the latest copy of this Policy. The Council revised this Policy on 13/03/2020 and updated section 8 to emphasise the controls needed in conjunction with working from home during the Covid-19 restrictions. The policy was again changed in September 2020 to reflect an expanded role for the Data and Information Champions in each Department to report compliance across a range of data protection headings to a new Data Protection Monitoring Committee.

Issue	Description of Change	Approval	Date of Issue
1	Initial issue	Draft	02/10/2018
2	Data Security	Draft	13/03/2020
	Compliance Reporting	Management Team	14/09/2020

12.3 A current version of this document is available to all members of staff on the Council's intranet site at the following location; Data Protection Policy

12.4 This Policy was approved by the Management Team on 14th September 2020 and is issued on a version controlled basis under the signature of the DPO.

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

13 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 the 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.

"Council" – Limerick City and County Council.

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

"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 Processing Agreement" – Article 28.3 of the GDPR requires that Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller. Article 28 also includes other particulars that must be stipulated in the data processing agreement.

"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 Nominee" - a nominated individual in each section of the Council, who will deal with data protection issues. In some cases there may be a "stand-in Data Protection Nominee" if the Data Protection Nominee is on leave.

"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 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.

"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, 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 Council from time to time.

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

"Privacy Statement/Notice" – A statement, for the benefit of data subjects, to comply with the transparency requirements of Articles 12 to 14 of the GDPR setting out information to be provided to the data subject where personal data are collected from the data subject and where personal data have not been collected from the data subject.

"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.

14 Schedule 2 -List of Council's Data Protection Policies

- General Data Protection Policy (this document).
- Response Policies and Procedures for Data Subject Requests
- Data Breach Policy
- CCTV Policy
- Policy on the use of Drones by Limerick City and County Council Staff