

Data Protection Policy
September 2019

Cooperative Learning Institute Ltd.
41 Marley Court,
Rathfarnham,
Dublin 14,
D14 E048.

Circulation Sheet

Client	Cooperative Learning Institute Limited
Project Title	The Cooperative Learning Institute Limited GDPR Project 2019
Document Title	Data Protection Policy

Revisions				
Rev	Status	Approved By	Office of Origin	Issue Date
R01	Release	Ark Services W: www.arkservices.ie	Cork	9 th September 2019

Circulation			
Name	Organisation	Method	Issue Date
Director	Cooperative Learning Institute Ltd	Email	9 th September 2019

Table of Contents

1	Introduction.....	5
2	Scope.....	5
3	GDPR Compliance Statement	6
4	GDPR Principles	7
4.1	Principle 1: Lawfulness, fairness and transparency.....	7
4.2	Principle 2: Purpose Limitation	7
4.3	Principle 3: Data Minimisation	7
4.4	Principle 4: Data Accuracy	7
4.5	Principle 5: Storage Limitation.....	7
4.6	Principle 6: Integrity & Confidentiality	7
4.7	Principle 7: Accountability	7
5	Data Subjects Rights	8
5.1	Rights of Data Subjects	8
5.2	Right of Access (Also known as a Subject Access Request)	8
5.3	Right to Rectification	8
5.4	Right to Erasure	8
5.5	Right to Restrict Processing.....	9
5.6	Right to Data Portability.....	9
5.7	Right to Object	9
5.8	Rights in Relation to Automatic Decision Making and Profiling.....	9
6	Responsibilities	10
6.1	Directors	10
6.2	Employees	10
6.2.1	General	10
6.3	Where The Cooperative Learning Institute Limited is the Data Controller	11
6.4	Where The Cooperative Learning Institute Limited is the Data Processor (School sharing personal data with us).....	11
7	Data Protection Policy	12
7.1	GDPR Awareness	12
7.2	Balance of Rights	12
7.3	Data Protection Impact Assessment.....	12
7.4	Lawful Processing Criteria	12
7.5	Storage and Use of Personal Data.....	12
7.6	Sharing Personal Data.....	13
7.7	Special Categories of Data.....	13
8	Data Processing Map & Retention Policy	14
8.1	Electronic Records	15
8.2	Training Records (Helping Hands Programme Attendees).....	17
8.3	Records Relating to Students in Schools	Error! Bookmark not defined.
8.4	Cooperative Learning Institute Limited Employee Personnel Files.....	18
8.5	Occupational Health Records.....	22
8.6	Superannuation / Pension / Retirement Records.....	24
8.7	Financial Records.....	25
9	Privacy Notices.....	27
9.1	When is a Privacy Notice required?.....	27
9.2	What needs to be included in a Privacy Notice?.....	27
9.3	What rights people have in relation to their own data?	27
10	Data Protection Communications	28
10.1	The Data Protection Policy	28
10.2	Privacy Notices.....	28
10.3	Website Privacy Notice.....	28
10.4	Data Privacy and employees	28
10.5	Communication plan for Privacy Notices	29

11	Third parties	30
11.1	General	30
11.2	Transfers of personal data to non-EEA jurisdictions.....	30
12	Data Security Breaches	31
12.1	Data Breach Action Plan	32
12.1.1	Identification and Initial Assessment of the Incident.....	32
12.1.2	Containment and Recovery	32
12.1.3	Risk Assessment	32
12.1.4	Notification.....	32
12.1.5	Evaluation and Response	32
13	Subject Access Requests (SARs)	33
13.1	Data Subject Rights.....	33
13.2	Logging Subject Access Requests	33
13.3	Responding to Subject Access Requests.....	33
13.4	Protecting Third Parties	33
14	Disposal of Personal Data	34
15	Governance Framework	35
15.1	Supervisory authority	35
15.2	Monitoring Compliance	35
15.3	Disciplinary Procedure.....	35
	Appendix 1: Subject Access Request Form	36
	Appendix 2: Website Privacy Notice	39
	Appendix 3: Staff Privacy Notice	41
	Appendix 4: Email Privacy Notice.....	43
	Appendix 5: Training Course Privacy Notice	44
	Appendix 6: Subject Access Request Register	45
	Acknowledgement of the Data Protection Policy	46

1 Introduction

The Cooperative Learning Institute Limited provides cutting edge knowledge, skills and tools for schools to ensure inclusion, wellbeing and psychological safety of students. Our programme provides a heat map that helps teachers access relationship dynamics hidden in the peer group. Vulnerable students can be identified before problems escalate or complaints are made allowing measures to assist them to be put in place.

Our award-winning programme has been developed through rigorous research and is based on international best practice and leading thinking. It provides a new approach, to identifying those students whose lives have become a silent and hidden torment.

Our training is supported by best in class software. The software element of our service can be used to assign students to classwork teams for optimally effective teamwork, ensuring that all students are included and that all are in teams where they feel wanted and welcome.

2 Scope

This policy states the commitment of the company to comply with the GDPR as both a Data Controller and Data Processor. It applies to the personally identifiable information of EU residents such as employees, students and staff involved in our programme as well as those attending events & training.

It applies directly to functions of The Cooperative Learning Institute Limited which collect or process personally identifiable information as part of normal operations. It also applies to external parties who act as Data Processors on behalf of Cooperative Learning Institute Limited.

3 GDPR Compliance Statement

The Cooperative Learning Institute Limited (“the company”) has at its core a desire to promote and protect the dignity and wellbeing of students. This policy is informed by these aspirations and also the General Data Protection Regulation of 2016 (GDPR). The policy applies to all directors, employees, the schools we work with including students and staff members, their parents/guardians, as well as applicants for positions within the organisation and service providers.

The Cooperative Learning Institute Limited is aware of its responsibilities as both a Data Controller & Data Processor of personal data under GDPR. The company has been briefed as to its scope and implications for the organisation. All employees at company who will be involved in processing personal information will be informed appropriately as to their responsibilities with respect to GDPR in their day to day work.

We are committed to high standards of data protection, information security & privacy. The Cooperative Learning Institute Limited respects the privacy of all and is committed to protecting their personal data.

We will safeguard the personal information under our remit and develop a robust data protection regime that is effective, fit for purpose and demonstrates compliance with the GDPR.

Our GDPR Principles:

- We will process all personal data fairly and lawfully;
- We will only process personal data for specified and lawful purposes;
- We will endeavour to hold relevant and accurate personal data, and where practical, we will keep this up to date;
- We will not retain personal data for longer than is necessary;
- We will keep all personal data secure;
- We will endeavour to ensure that personal data is not transferred to countries outside of the European Economic Area (‘EEA’) without adequate protection.

The detailed arrangements for achieving these objectives are set out in the main body of this policy.

The Cooperative Learning Institute Limited is committed to upholding the standards outlined in this policy. Sufficient authority and resources, both financial and otherwise, will be made available to enable the business to carry out their responsibilities under the GDPR. All employees will be made aware of and have access to this policy.

The Policy will be reviewed annually in light of experience and future developments within the organisation.

Signed: _____
CEO & Director

Date: _____

4 GDPR Principles

4.1 Principle 1: Lawfulness, fairness and transparency

The Cooperative Learning Institute Limited believes in operating our organisation fairly and ethically and this will extend to all personal data held for those purposes. Data Subjects will be informed when data is being collected, and at the same time informed what we will use that data for. We will ensure that appropriate technical and organisational measures are in place to secure that data.

Collection and processing of data will be transparent. Privacy notices relating to data rights will be published as appropriate in plain English and will be structured where relevant to improve accessibility of this information to data subjects. Persons will be clearly advised of their rights also.

4.2 Principle 2: Purpose Limitation

Personal data collected by The Cooperative Learning Institute Limited will be processed only for the purpose for which it was collected. In the event that this purpose should change, data subjects will be informed within the 30-day regulatory period and consent sought for the change.

4.3 Principle 3: Data Minimisation

The Cooperative Learning Institute Limited will collect only the minimum quantity of personal data to carry out a particular task. Where appropriate, potential data subjects will be requested not to provide unwanted or inappropriately sensitive personal information.

4.4 Principle 4: Data Accuracy

The Cooperative Learning Institute Limited will make every effort to ensure that data subjects' information is accurate and up to date. The Cooperative Learning Institute Limited will endeavour to ensure via appropriate levels of training that it is transcribed accurately. If it is not possible for subjects to correct their data personally, data can be corrected by contacting Reception.

4.5 Principle 5: Storage Limitation

The Cooperative Learning Institute Limited will store and retain personal data only while there is a valid and lawful basis to do so. Personal information will be deleted when it is no longer required for the purposes for which it was collected.

Where systems do not allow deletion of all records relating to an individual, records will be anonymised by "hashing" personal information fields with substituted generic text.

4.6 Principle 6: Integrity & Confidentiality

Personal Data shall be processed securely i.e. in a manner that ensures appropriate security of the Personal Data, including protection against unauthorised or unlawful processing, accidental loss, destruction or damage. The Cooperative Learning Institute Limited will use appropriate technical and organisational measures to ensure the integrity and confidentiality of personal data is maintained at all times.

4.7 Principle 7: Accountability

The Cooperative Learning Institute Limited is responsible for and is able to demonstrate compliance with GDPR. This means The Cooperative Learning Institute Limited will demonstrate that these Data Protection Principles (as outlined here) are met for all Personal Data for which it is responsible.

5 Data Subjects Rights

5.1 Rights of Data Subjects

The Cooperative Learning Institute Limited recognises the following as the rights of Data Subjects in certain circumstances:

- The right to make Subject Access Requests (SARs);
- The right to have inaccuracies corrected (rectification);
- The right to have information erased (right of erasure);
- The right to restrict the processing of information (restriction);
- The right to be informed on why personal data is processed (notification);
- The right to Data Portability;
- The right to object to processing of personal data (object);
- The right not to be subject to decisions based on automated decision making.

5.2 Right of Access (Also known as a Subject Access Request)

Data Subjects have the Right to obtain:

- Confirmation that their data is being processed;
- Access to their personal data;
- Other supplementary information;

Subject Access Requests must be responded to within one month through the Director. See Section 12 for the procedure.

5.3 Right to Rectification

Data Subjects are entitled to have their personal data rectified if it is inaccurate or incomplete. If the information in question has been disclosed to a third party the Data Controller must inform them of the request for rectification where possible. The Data Subject is also entitled to be informed of the third parties to whom the data has been disclosed, where appropriate.

Rights to rectification must be responded to within one month. See Section 12 for the procedure.

5.4 Right to Erasure

This Right is also known as the 'Right to be Forgotten'. It enables Data Subjects to request the deletion or removal of personal data where there is no compelling reason for its continued processing by the Data Controller.

The Right to Erasure applies in the following circumstances:

- The personal data is no longer necessary in relation to the purpose for which it was originally collected;
- The processing was based on consent, and the Data Subject has now withdrawn their consent;
- The Data Subject objects to processing and there is no overriding legitimate interest of the Data Controller;
- The data was being unlawfully processed;
- The data must be erased to comply with a legal obligation;

On receipt of this request, we will carry out an assessment of whether the data can be erased without affecting the ability of this company / the client (school) / Department of Education to provide future services to the Data Subject or to meet its statutory obligations.

5.5 Right to Restrict Processing

The Right to Restrict Processing applies in the following circumstances:

- When a Data Subject contests the accuracy of their personal data, then processing should be restricted to storage only until accuracy is verified;
- When a Data Subject objects to processing which is being carried out for the reason of performance of a task in the public interest, then the Data Controller must restrict processing to storage only whilst they consider whether their lawful basis for processing override the Rights and freedoms of the individual;
- When processing is unlawful and a Data Subject opposes the use and requests restriction to storage instead;
- When the Data Controller no longer needs the personal data but the Data Subject requires it for the purpose of, or in the defence of a legal claim.

When this Right is exercised, The Cooperative Learning Institute Limited will carry out an assessment of whether the data can be restricted without affecting the ability of the company / the client (school) / Department of Education to provide future services to you.

5.6 Right to Data Portability

This Right allows individuals to obtain and reuse their personal data for their own purposes across different services. It allows the individual to move, copy or transfer personal data easily from one service provider to another in a safe and secure way in a common data format e.g. pdf file.

The Right to Data Portability applies in the following circumstances:

- When the personal data was provided to the controller directly by the Data Subject;
- Where the processing is based on consent or performance of a contract;
- When processing is carried out by automated means.

5.7 Right to Object

Individuals have the Right to object to processing based on:

- Legitimate interest or performance of a task in the public interest/exercise of official authority (including profiling);
- Direct marketing (including profiling);
- Processing for the purposes of scientific/historical research and statistics.

5.8 Rights in Relation to Automatic Decision Making and Profiling

This Right provides safeguards for individuals against the risk that a potentially damaging decision is taken without human intervention. The Right not to be subject to a decision applies when:

- It is based on automated processing;
- It produces legal/significant effects on the individual;
- Is necessary for entering into or performance of a contract or authorised by law;
- Is based on explicit consent;
- Does not have a legal/significant effect on the data subject.

At present, automated processing is not performed.

6 Responsibilities

6.1 Directors

- Ensure the policy is communicated & implemented throughout the company;
- Ensure personal data is collected and processed in accordance with this policy;
- Ensure that the basic principles of data protection are explained to employees when commencing work at the company;
- Ensure that there are regular updates to data protection awareness, so that data protection is a “living” process aligned to the organisation’s ethos.
- Periodically check data held regarding accuracy.
- Driving privacy and data protection awareness in the organisation;
- Identifying training needs and arranging for refresher training sessions as needed;
- Taking appropriate preventative actions to mitigate the risk of data breaches arising;
- Spearheading the response to any data breach (following the data breach protocol);
- Due diligence of service providers (data processors) prior to any service provider being retained including ensuring appropriate written contracts in place with all service providers;
- Ensure that Record-keeping of data protection items is carried out;
- Periodic reviews of all data protection arrangements are carried out.

6.2 Employees

6.2.1 General

- Adhere to the values and standards set forth in this Policy and comply with relevant procedures. Request clarification if there is uncertainty. Read and sign acknowledgement of this policy;
- Correcting Personal Data known to be incorrect, inaccurate, incomplete, ambiguous, misleading or outdated, even if the Data Subject does not request rectification;
- Keeping Personal Data only as per the Retention Policy to satisfy the permitted uses;
- Ensure any personal data is accurately processed in accordance with this policy;
- Keep the company office clean and tidy;
- Ensure that personal data is not visible to others (e.g. leaving files on desk, computers left logged into);
- Keep personal data out of sight of visitors to the office;
- Diligence and attention-to-detail when entering data on to any work related administrative system;
- Ensuring that passwords for accessing software systems are appropriate i.e. 8-12 characters, mixture of upper case / lower case / numbers and symbols;
- Keep data accurate, complete, and up-to-date;
- Ensuring filing cabinets and the office door is kept locked when not in use;
- Respect access-permission levels, never looking into files/records to which you have no genuine employment reason for accessing, adhering to the principle of “need to know”;
- Immediately notify the relevant Director if anyone attempts to obtain unauthorised access to personal data;

6.3 Where The Cooperative Learning Institute Limited is the Data Controller

Implement appropriate technical and organisational measures and be able to demonstrate that data processing is performed in accordance with the Regulation; review and update those measures where necessary considering at all times (with regard to the processing of personal data):

- Lawfulness, fairness and transparency;
- Purpose limitation;
- Data minimisation;
- Accuracy;
- Storage limitation;
- Integrity and confidentiality;

6.4 Where The Cooperative Learning Institute Limited is the Data Processor (School sharing personal data with us)

- We will only process personal data on documented instructions from the controller (i.e. the school), including with regards to transfers of data outside the EEA;
- We will ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- We will take all measures pursuant to Article 32 on security of processing;
- We will respect the conditions for enlisting another processor or sub-processor;
- We will assist the controller by appropriate technical and organisational measures for the fulfilment of the controller's obligation to respond to requests to exercise data subjects' rights. This may include:
 - Pseudonymisation and encryption of data;
 - The ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
 - A process for regularly testing, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.
- We will assist the controller in complying with the obligations in Articles 32–36 (security, data protection impact assessments and breach notification), considering the nature of the processing;
- We on written instruction from the controller, delete or return all personal data to the controller after the end of the provision of data processing services; and
- Make available to the controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

7 Data Protection Policy

7.1 GDPR Awareness

The Cooperative Learning Institute Limited will ensure that all employees are aware of GDPR and are trained appropriately to their duties in respect of processing of personal data as per this data protection policy. The training and awareness programme will consist of:

- Briefing to all employees;
- A general email to all employees with the Data Protection Policy;

7.2 Balance of Rights

In processing personal data for the operation of the organisation, we will ensure that we will only use a subject's data if the subject's rights do not outweigh our lawful basis in using that data.

The balance will be assessed by first checking that we have a lawful basis for using the data, and then evaluating whether disproportionate financial, reputational or social harm could be caused to the individual through our use of their data. We will achieve this on an ongoing basis via the Data Protection Policy and Record of Processing methods already explained in this policy.

7.3 Data Protection Impact Assessment

The Cooperative Learning Institute Limited will carry out and record an impact assessment appropriate in scope to the sensitivity of the personal data being processed. This will identify risks to the data subject, to compliance and to the organisation with respect to GDPR principles. This exercise will be repeated as required i.e. when a change in practices causes us to re-evaluate the impact on data privacy.

7.4 Lawful Processing Criteria

The Cooperative Learning Institute Limited processes personal data in the pursuance of several lawful processing criteria. In all cases we examine the balance of rights with respect to the use of personal data. It is our objective to align our activities with the rights of the data subject, such that our use of their data is beneficial to the data subject and that any inconvenience or risk to the data subject is minimal in comparison with the benefits there from. We have established our lawful processing criteria in the Data Map & Processing Activities in Section 8.

7.5 Storage and Use of Personal Data

The security of personal data is a very important consideration under the GDPR and is taken very seriously at Cooperative Learning Institute Limited. Appropriate security measures will be taken by the organisation to protect unauthorised access to this data. A minimum standard of security will include the following measures:

- Access to the information will be restricted to authorised employees on a "need-to-know" basis;
- Manual files will be stored in a relevant filing system, located away from public areas in locked cabinets;
- Computerised data will be held in secure databases (password protected);
- Any information which needs to be disposed of will be done so carefully and thoroughly;

7.5.1 Paper based records

Paper based records shall be kept in a secure place where unauthorised people cannot access it. This also applies to data that is usually stored electronically but has been printed out for a valid reason:

- All personnel will ensure that personal data, paper and printouts are not left where unauthorised people could see them;
- When not required, the paper or files will be kept in a relevant filing system in a locked secured filing cabinet or;
- Scanned, transferred to and saved on a password protected computer;
- Data will be shredded and disposed of securely.

7.5.2 Electronic records

When data is stored electronically, it will be protected from unauthorised access, accidental deletion and malicious hacking attempts:

- Data will be protected by strong passwords that are changed regularly and never shared between employees;
- Personal Data will only be stored on equipment supplied by the company i.e. desktop computers / laptops;
- Computers containing personal data will be sited in a secure location;
- Data will be backed up frequently;
- All computers containing data will be protected by approved security software and a firewall.

7.5.3 Use of Personal Data

We will only process data to accomplish specified, explicit, and legitimate purposes. We will not process beyond such purposes unless further processing compatible for original purpose data was collected. We use personal data originating from either the company or our clients for purposes including:

- provision of training and support to our clients;
- provision of our proprietary sociometric tool to our clients;
- to comply with our contractual obligations to our clients;
- to promote our legitimate business interests;
- to comply with our legal obligations as limited company;
- to comply with our reporting obligations to various government bodies i.e. CRO, Revenue;
- to provide appropriate training, direction and support to our staff;

7.6 Sharing Personal Data

From time to time, we may share personal data with An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc. The sharing of personal data and the nature of what is shared depends on various factors. We also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed.

7.7 Special Categories of Data

7.7.1 Children/Students

Special categories of particularly sensitive personal information requires higher levels of protection and includes data relating to race, ethnic origin, politics, religion, trade union membership, genetics, biometrics (where used for ID purposes), health, sex life, sexual orientation.

We do not process special categories of data.

8 Data Processing Map & Retention Policy

Everyone who works for The Cooperative Learning Institute Limited has a responsibility for ensuring data is collected, stored, and handled appropriately. Each person who handles personal data must ensure that it is handled and processed in line with this policy and the data protection principles.

Personal Data processed at The Cooperative Learning Institute Limited is summarised in the Data Map along with our legal justification for processing this data and our Retention Policy for same.

Data maps have been prepared to identify our data processing activities. Employees should refer to the Data Map to ensure that personal is stored correctly as per the policy. This shows what data collected, where it is stored, and how it is used.

8.1 Electronic Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D01 Sociometric Software Application	Restricted	Microsoft Azure	Performance of Contract.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Teacher Name, Student Name, Class, Sociometric findings.	Authorised Staff Members. Results shared with authorised members of the school care team.	See policy from Microsoft https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located . Note all data transfers are governed by this: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46	Up to 30 days post contract expiration.	Hashed Database.	Technical: Individual Logins for authorised staff members. Authentication by Microsoft using username and password. Access to DB over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL) technology that encrypts mail for secure delivery. Data Stored in EU always. Each Microsoft® Data Center is ISO 27001 certified. Up to 30 days Point in Time Restore is designed for recovering a database from a recent backup after accidental data corruption or deletion. Organisational: Relevant employees trained on the Data Protection Policy. Paper records are filed and stored in secure locked cabinets to which only designated employees have access to. Computers on which records are accessible are password protected and are accessible only to designated employees. Office is locked when not in use.
D02 Office Applications including Outlook, Word, Excel etc.	Restricted	Local Computer	Emails & Cloud Server in the normal business of the organisation.	Legitimate Interests.	Personal Data incl. Student Data, Employee Data, Policies & Procedures.	Authorised Staff Members.	See policy from Microsoft https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located . Note all data transfers are governed by this: http://www.microsoftvolumelicensing.com/DocumentSearch.aspx?Mode=3&DocumentTypeId=46	Indefinitely.	N/a	Technical: Individual Logins for Employees. Authentication by Microsoft using username and password. Access to Email over Encryption / Https / TLS. TLS is an industry-wide standard based on Secure Sockets Layer (SSL) technology that encrypts mail for secure delivery. Organisational: Relevant employees trained on the Data Protection Policy. Paper records are filed and stored in secure locked cabinets to which only designated employees have access to. Computers on which records are accessible are password protected and are accessible only to designated employees. Office is locked when not in use.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D03 Website	Confidential	Hosting Provider.	Provide information to the public.	Legitimate Interests.	Personal Data incl. Photos of Academic Achievement Awards, Retirements etc.	Anyone visiting our website.	N/a	Indefinitely.	N/a	<p>Technical: Individual Logins for Employees. Authentication by using username and password. Access to Server over Encryption / Https / TLS.</p> <p>Organisational: Relevant employees trained on The Data Protection Policy.</p>

8.2 Training Records (Helping Hands Programme Attendees)

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D04 Attendees Information	Confidential	Paper: Company Office in locked filing cabinets.	Fulfil processing of training records in the course of delivering training.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Name; Surname; Phone Number; Email Address;	Trainers. Authorised members of staff.	N/a	2 years after course takes place.	Confidential Shredding.	<p>Technical: Only the minimum data is collected from the data subject to fulfil our processing needs.</p> <p>Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.</p>
D05 Registers of Training	Confidential	Paper: Company Office in locked filing cabinets.	Fulfil processing of training records in the course of delivering training.	Legitimate Interests. Contractual Obligation.	Personal Data incl. Name; Surname; Phone Number; Email Address;	Trainers. Authorised members of staff.	N/a	2 years after course takes place.	Confidential Shredding.	<p>Technical: Only the minimum data is collected from the data subject to fulfil our processing needs.</p> <p>Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.</p>

8.3 Cooperative Learning Institute Limited Employee Personnel Files

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D011 Applications, qualifications, references, recruitment, job specification, contract etc. D017 Application &/CV D018 Qualifications D019 References D020 Interview: database of applications (the section which relates to the employee only) D021 Selection Criteria D022 Interview Board Marking Scheme & Boards Notes	Confidential	Paper: Company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D023 Job Specification / Description	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D024 Contract/ Conditions of employment										
D025 Probation letters/forms										
D026 Leave of absence applications										
D027 Job Share										
D028 Career Break										
D029 Paternity / Maternity Leave	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D030 Force Majeure Leave	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D031 Carer's Leave	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D032 Working Time Act (attendance hours, holidays, breaks)	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D033 Allegations / Complaints	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D034 Grievance and Disciplinary records	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

8.4 Occupational Health Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D035 Sickness Absence Records / Certificates	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	<p>Technical: Only the minimum data is collected from the data subject to fulfil our processing needs.</p> <p>Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.</p>
D036 Pre-Employment Medical Assessment										
D037 Occupational Health Referral										
D038 Correspondence regarding retirement on ill-health grounds										
D039 Accident / Injury at Work Reports	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract. Defence of Legal Claim.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years.	Paper Copies: Confidential Shredding.	<p>Technical: Only the minimum data is collected from the data subject to fulfil our processing needs.</p> <p>Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.</p>

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D040 Medical assessments or referrals	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D041 Sick Leave Records (Sick Benefit Forms)	Confidential	Paper: company Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff.	N/a	Retain for duration of employment plus 7 years There is a statutory requirement to retain for 3 years.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

8.5 Superannuation / Pension / Retirement Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D042 Records of previous service (incl. correspondence with previous employers)	Confidential	Paper: Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff.	N/a	Indefinitely.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D043 Pension Calculation	Confidential	Paper: Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff.	N/a	Indefinitely.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.
D044 Salary Claim Forms	Confidential	Paper: Office in locked filing cabinets.	HR activities of the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff.	N/a	Duration of employment + 7 years or for the life of employee/ former employee plus + 7 years - whichever is the longer.	Paper Copies: Confidential Shredding.	Technical: Only the minimum data is collected from the data subject to fulfil our processing needs. Organisational: Office is locked when not in use. Filing cabinets holding these records will be locked at the end of each day. Computers on which records are stored are password protected and are accessible only to designated employees. Relevant employees briefed on the Data Protection Policy.

8.6 Financial Records

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D045 Accounts	Confidential	Paper: Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff. Auditors.	N/a	7 Years.	Confidential Shredding.	<p>Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection.</p> <p>Note: The DES requires of schools that “pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system.</p> <p>Organisational: Access to Financial Records is limited to authorised personnel i.e. Director / Deputy Director, Admin Team.</p>
D046 Payroll and Taxation	Confidential	Paper: Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff. Auditors.	N/a	7 Years.	Confidential Shredding.	<p>Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection.</p> <p>Note: The DES requires of schools that “pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system.</p> <p>Organisational: Access to Financial Records is limited to authorised personnel i.e. Director / Deputy Director, Admin Team.</p>

Dataset	Classification	Location Stored	Purpose of Processing	Lawful Basis for Processing	Categories of Personal Data	Categories of Recipients	Safeguards (Transfer to 3 rd Countries)	Max. Data Retention Period	Final Disposal	Description of Technical and Organisational Security Measures
D047 Invoices / Back Up Records / Receipts	Confidential	Paper: Office in locked filing cabinets.	Maintain good accounting records for the organisation.	Legal Obligation. Fulfilment of Contract.	Personal Data incl. Application Forms. CV. Name. Address. Qualifications. Teacher Council Number. Email. Career History.	Authorised members of staff. Auditors.	N/a	7 years.	Confidential Shredding.	<p>Technical: Revenue Commissioners require that records be kept for at least six years after the end of the tax year. Records must be made available for inspection by authorised officers of the Revenue Commissioners or of the Dept. of Social Protection.</p> <p>Note: The DES requires of schools that "pay, taxation and related school personnel service records should be retained indefinitely within the school. These records can be kept either on a manual or computer system.</p> <p>Organisational: Access to Financial Records is limited to authorised personnel i.e. Director / Deputy Director, Admin Team.</p>

9 Privacy Notices

9.1 When is a Privacy Notice required?

Where information is being collected directly from an individual, a Privacy Notice will be provided at the point at which the data is collected.

- Where information is obtained from another source, a Privacy Notice must be provided:
- If personal data is to be used to communicate with the data subject, at the latest at the time of the first communication with the data subjects;
- If disclosure to another recipient is envisaged, at the latest when personal data is first disclosed.

9.2 What needs to be included in a Privacy Notice?

Privacy Notices will contain specific information which informs data subjects of:

- Who is collecting the data;
- Why it is being collected;
- What legal basis is being relied upon to process the data;
- How it will be processed;
- How long it will be kept for;
- Who it will be disclosed to.

9.3 What rights people have in relation to their own data?

Individuals will also be made aware of their rights as per Section 5.

- The right to make Subject Access Requests (SARs).
- The right to have inaccuracies corrected (rectification).
- The right to have information erased (right of erasure).
- The right to restrict the processing of information (restriction).
- The right to be informed on why personal data is processed (notification).
- The right to Data Portability.
- The right to object to processing of personal data (object).
- The right not to be subject to decisions based on automated decision making.

10 Data Protection Communications

10.1 The Data Protection Policy

This document will be made known to all employees as the primary source of Data Protection Policy at Cooperative Learning Institute Limited.

10.2 Privacy Notices

Cooperative Learning Institute Limited's main method of informing data subjects and the general public regarding our use of their data is the Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of The Cooperative Learning Institute Limited as the controller / processor as appropriate of personal data;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subjects' rights as observed by Cooperative Learning Institute Limited;

The Privacy Notice will be formatted appropriately for the medium in which it is published.

The Privacy Notice is considered an advisory notice regarding The Cooperative Learning Institute Limited policy, and is not intended to constitute a contract with any person.

10.3 Website Privacy Notice

Cooperative Learning Institute Limited's main method of informing data subjects and the general public regarding its use of their data whilst on our website will be the Website Privacy Notice. The Privacy Notice will include at a minimum:

- Identification of The Cooperative Learning Institute Limited as the controller / processor as appropriate of personal data;
- A description of the personal information we hold and use;
- An explanation of what we use the information for;
- Who we share the information with;
- Where we store the information;
- How long we keep the information;
- A summary of the data subject's rights as observed by Cooperative Learning Institute Limited;
- Summary technical details regarding information processing (including cookie use);

The Privacy Notice will be formatted appropriately for the medium in which it is published.

The Privacy Notice is considered an advisory notice regarding The Cooperative Learning Institute Limited policy and is not intended to constitute a contract with any person.

10.4 Data Privacy and employees

Employees will be formally notified of Cooperative Learning Institute Limited's position with respect to this policy via a briefing.

10.5 Communication plan for Privacy Notices

The Cooperative Learning Institute Limited will ensure that employees and external parties are informed regarding our use of their data. Any subsequent changes to our policy or practices which affect how user's data is processed will be communicated as per this section.

Employees will be informed directly by email informing of the change, and with attachments or links to supplementary information where required.

Cooperative Learning Institute Limited's main vehicle for informing the public of our privacy policy is the Privacy Notice which is published on our website. This will be revised as necessary to ensure compliance.

Where certain classes of users (e.g. students) need to be informed more proactively regarding our use of their personal data, we will accomplish this by informing them through their school. This will be carried out in advance of the change going live. Where a change of use requires a response, the lack of a response will not be treated as acceptance.

From time to time it will be necessary to revise the Data Protection Policy as well as associated Privacy Notice in response to changes in regulations or evolution of expectations for compliance.

The Privacy Notice itself contains an advisory to users to check regularly for changes.

11 Third parties

11.1 General

The Cooperative Learning Institute Limited avails of the services of outside parties who act as Data Processors on our behalf to assist us in essential organisation processes.

These include but are not limited to Finance, Payroll, Software & IT functions.

The Cooperative Learning Institute Limited will perform due diligence with respect to any and all such third parties and ensure that:

- The basis of the relationship is clearly defined and falls under this Data Protection Policy;
- A Data Processing Agreement is in place that strengthens our compliance with the GDPR;
- Where data held may not come under GDPR, that a non-disclosure agreement protects personal data;

Only providers who are actively involved in processing personal data will come under scrutiny.

11.2 Transfers of personal data to non-EEA jurisdictions

Our use of third parties may include entities outside the EU/EEA who will process personal data of EU residents on our behalf in the direct exercise of our key organisational processes. The Cooperative Learning Institute Limited warrants that the use of non-EEA services is a organisational necessity. In these cases, The Cooperative Learning Institute Limited has identified the following:

Processor	Stored in the EU/EEA?	EU/US Privacy Shield Agreement in place
Microsoft	Not always	Yes
Mongo DB	Not always	Yes

12 Data Security Breaches

Where an incident gives rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data, in manual or electronic form, The Cooperative Learning Institute Limited will give immediate consideration to informing those affected. Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures. In appropriate cases, The Cooperative Learning Institute Limited will also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, our Schools, An Garda Síochána, Department of Education etc.

If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it, The Cooperative Learning Institute Limited may conclude that there is no risk to the data and therefore no need to inform data subjects. Such a conclusion would only be justified where the technological measures (such as encryption) were of a high standard.

All incidents of loss of control of personal data in manual or electronic form by a data processor must be reported to The Cooperative Learning Institute Limited as soon as the data processor becomes aware of the incident. Conversely, where the Cooperative Learning Institute Limited is the processor, it too will report the loss of control to the relevant Data Controller.

All incidents in which personal data has been put at risk should be reported to the Office of the Data Protection Commissioner (DPC) as soon as the organisation becomes aware of the incident, except when the full extent and consequences of the incident has been reported without delay directly to the affected data subject(s) and it affects no more than 100 data subjects and it does not include sensitive personal data or personal data of a financial / sensitive personal nature. If there is any doubt related to the adequacy of technological risk-mitigation measures then The Cooperative Learning Institute Limited will report the incident to the DPC.

The Cooperative Learning Institute Limited will make initial contact with the DPC within 72 Hours of becoming aware of the incident, outlining the circumstances surrounding the incident. This initial contact will be through their website - <https://forms.dataprotection.ie/contact>. The DPC will make a determination regarding the need for a detailed report and/or subsequent investigation based on the nature of the incident and the presence or otherwise of appropriate physical or technological security measures to protect the data.

Should the DPC request the company to provide a detailed written report of the incident, The Cooperative Learning Institute Limited will specify a timeframe for the delivery of the report based on the nature of the incident and the information required. Such a report should reflect careful consideration of the following elements:

- the amount and nature of the personal data that has been compromised;
- the action being taken to secure and / or recover the personal data that has been compromised;
- the action being taken to inform those affected by the incident or reasons for the decision not to do so;
- the action being taken to limit damage or distress to those affected by the incident;
- a chronology of the events leading up to the loss of control of the personal data;
- and the measures being taken to prevent repetition of the incident.

Depending on the nature of the incident, the DPC may investigate the circumstances surrounding the personal data security breach. Investigations may include on-site examination of systems and procedures and could lead to a recommendation to inform data subjects about a security breach incident where the company has not already done so. If necessary, the DPC may use their enforcement powers to compel appropriate action to protect the interests of data subjects.

Even where there is no notification of the DPC, The Cooperative Learning Institute Limited will keep a summary record of each incident which has given rise to a risk of unauthorised disclosure, loss, destruction or alteration of personal data. The record should include a brief description of the nature of the incident and an explanation of why the company did not consider it necessary to inform the DPC. Such records should be provided to the DPC upon request.

12.1 Data Breach Action Plan

12.1.1 Identification and Initial Assessment of the Incident

- Identify and confirm volumes and types of data affected;
- Establish what personal data is involved in the breach;
- Identify the cause of the breach;
- Estimate the number of data subjects affected;
- Establish how the breach can be contained;

12.1.2 Containment and Recovery

- Establish who within the organisation needs to be made aware of the breach;
- Establish whether there is anything that can be done to recover the losses and limit the damage the breach could cause;
- Partial or complete systems lockdown;
- Establish if it is appropriate to notify affected individuals immediately (for example where there is a high level of risk of serious harm to any individual);

12.1.3 Risk Assessment

- A detailed analysis of volumes and types of data involved will be undertaken and a risk assessment carried out to establish and the risk to data subjects;

12.1.4 Notification

- On the basis of the evaluation of risks and consequences, the Director will decide whether it is necessary to notify relevant stakeholders i.e.
 - the Gardaí;
 - the Data Subjects affected by the breach;
 - the Data Protection Commissioner;
 - the Cooperative Learning Institute Limited's Insurers;
- In accordance with the Data Protection Commissioner's Code of Practice all incidents in which Personal Data has been put at risk will be reported to the Office of the DPC within 72 hours of the company first becoming aware of the breach.
- If, following the assessment described above, it is established that the data breach has been fully and immediately notified to the Data Subjects affected and it affects no more than 100 Data Subjects and it does not include sensitive personal data or personal data of a financial nature, it may not be required to be notified to the DPC. This will be assessed on an individual basis according to the Data Protection Policy on Data Breach above, and where there is any doubt, legal advice will be sought.

12.1.5 Evaluation and Response

- Following any serious Breach of Data incident, a thorough review will be undertaken by the response team and a report will be made to the Board of Management. This will identify the strengths and weakness of the process and will indicate what areas may need to improve.
- Response may also include updating the Data Protection Policy and retraining employees.

13 Subject Access Requests (SARs)

13.1 Data Subject Rights

Data Subjects are entitled to obtain, based upon a request made in writing to The Cooperative Learning Institute Limited using the 'Subject Access Request Form' and upon successful verification of their identity, the following information about their own Personal Data:

- The purposes of the collection, processing, use and storage of their Personal Data.
- The source(s) of the Personal Data, if it was not obtained from the Data Subject;
- The categories of Personal Data stored for the Data Subject.
- The recipients or categories of recipients to whom the Personal Data has been or may be transmitted, along with the location of those recipients.
- The envisaged period of storage for the Personal Data or the rationale for determining the storage period.
- The right of the Data subject to:
 - object to Processing of their Personal Data.
 - lodge a complaint with the Data Protection Authority.
 - request rectification or erasure of their Personal Data.
 - request restriction of Processing of their Personal Data.

13.2 Logging Subject Access Requests

All requests received for access to or rectification of Personal Data will be directed to the Director, who will log each request as it is received using the Appendix 6: Subject Access Request Register. The data subject will be asked to fill out the Appendix 1: Subject Access Request Form.

13.3 Responding to Subject Access Requests

A response to each request will be provided within 30 days of the receipt of the written request from the Data Subject.

Appropriate verification must confirm that the requestor is the Data Subject or their authorised legal representative. Data Subjects shall have the right to require The Cooperative Learning Institute Limited to correct or supplement erroneous, misleading, outdated, or incomplete Personal Data.

If the company cannot respond fully to the request within 30 days, the organisation shall nevertheless provide the following information to the Data Subject, or their authorised legal representative within the specified time:

- An acknowledgement of receipt of the request.
- Any information located to date.
- Details of any requested information or modifications which will not be provided to the Data Subject, the reason(s) for the refusal, and any procedures available for appealing the decision.
- An estimated date by which any remaining responses will be provided.
- The name and contact information of The Cooperative Learning Institute Limited individual who the Data Subject should contact for follow up.

13.4 Protecting Third Parties

It should be noted that situations may arise where providing the information requested by a Data Subject would disclose Personal Data about another individual. In such cases, information must be redacted or withheld as may be necessary or appropriate to protect that person's rights.

14 Disposal of Personal Data

The Cooperative Learning Institute Limited will conduct a regular review of the personal data they hold for the purpose of disposing of redundant personal data. Such a review should take place on an annual basis. Such a review should involve the following steps:

1. Identification of records (both electronic and paper) which contain personal data or sensitive personal data (see Data Map & Retention Policy in Section 8);
2. Identification of the purpose(s) for which the data was originally obtained i.e. why did we collect the data (see Data Map & Retention Policy in Section 8);
3. Appraisal of the records to determine if they contain personal data which is no longer necessary for the purposes for which it was originally obtained: This step will involve:
 - a. Consulting the Retention period as outlined in the Data Map & Retention Policy in Section 8.
 - b. Identifying the records for disposal.
 - c. Obtain permission from the Director to dispose of the records.
 - d. Document the disposal of records.
4. Suitable third-party service provider should be contacted to provide a secure erasure and destruction service i.e. confidential shredding through a certified data destruction specialist.
5. Consultation should also take place with the Director for advice on record retention periods and to ensure that records are disposed of in a safe, secure and appropriate manner.

15 Governance Framework

15.1 Supervisory authority

The Irish Data Protection Commission is our lead supervisory authority under GDPR.

15.2 Monitoring Compliance

The Cooperative Learning Institute Limited will carry out internal GDPR compliance audits against our policy and procedures.

We will also arrange audits of our compliance by independent third parties at longer intervals.

All audit records will remain confidential to The Cooperative Learning Institute Limited and will be shown only to regulatory authorities on request. Each audit will, as a minimum, assess:

- Compliance with Data Protection Policy in relation to the protection of Personal Data, including:
 - The assignment of responsibilities;
 - Raising awareness;
 - Training of Employees;
- The effectiveness of Data Protection related operational practices, including:
 - Data Subject rights;
 - Personal Data incident management;
 - Personal Data complaints handling;
- The level of understanding of Data Protection Policies and Privacy Notices;
- The currency of Privacy Notices.
- The accuracy of Personal Data being stored.
- The conformity of Data Processor activities.

15.3 Disciplinary Procedure

Breaches of the GDPR or the company Data Protection Policy may be treated as a matter for discipline and depending on the seriousness of the breach and will be dealt with by the Director in accordance with the company Disciplinary Procedure.

For breaches of the GDPR Regulations, which do not warrant such action, the employee will be advised of the issue and given a reasonable opportunity to put it right.

In the case of contractors or external service providers, serious breaches of the policies and procedures can and will be deemed grounds for termination of contractual agreements.

Appendix 1: Subject Access Request Form

Section 1 – Your details (PLEASE USE BLOCK CAPITALS)

Surname:	
First Name(s):	
Previously known as (if applicable):	
Address:	
Date of birth:	
Telephone number:	
Email address:	

SECTION 2 – Your relationship with Cooperative Learning Institute Limited

Are you a current/former* employee?	YES / NO
If yes, please provide the following details: Period which you were an employee in The Cooperative Learning Institute Limited i.e. Month & Year.:	
Are you a current/former client of The Cooperative Learning Institute Limited?	YES / NO
If yes, please provide the following details: Period which you were a client of The Cooperative Learning Institute Limited:	
If neither, please indicate your relationship with the Cooperative Learning Institute Limited including dates:	

SECTION 3 – PERSONAL DATA REQUESTED

In the box below, please provide as much detail as you can about the personal data you wish to access in order to help us locate it quickly.

In accordance with the GDPR, I request access to the following personal data that I believe The Cooperative Learning Institute Limited holds about me:

SECTION 4 – FEES

No application fees are required for Subject Access Requests
--

SECTION 5 - IDENTIFICATION

In order for us to protect the security of personal data, it is necessary for you to provide proof of your identity. Two forms of identification must accompany this form. Acceptable forms of identification include:

- Copy of passport or driving licence
- Copy of bank statement
- ID Card
- Copy of utility bill

Copies are acceptable in most cases; however, we reserve the right to ask to see original documents where necessary. Copies of such documents sent with your access request form will be securely destroyed once we have verified your identity.

Please complete either section 6 or section 7 as appropriate

SECTION 6 - DECLARATION OF DATA SUBJECT

I confirm that I am the data subject named in Section 1 and I am requesting access to my own personal data. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.

Signed:

Date:

SECTION 7 - DECLARATION OF DATA SUBJECT FOR AGENT TO ACT ON THEIR BEHALF

If you wish someone else to submit a data access on your behalf (e.g. family member, solicitor) please complete this section.

I confirm that I am the data subject named in Section 1. I give permission for the person or organisation named below to act on my behalf in relation to my subject access request. I have enclosed evidence of my identity referred to in Section 5 and confirm that I want my personal data to be sent to my representative at the address below. I understand that the information I have supplied will be used to confirm my identity and help locate the information I have requested. I also understand that it may be used for statistical and monitoring purposes.

Signed:

Date:

Name of agent:

Relationship to data subject:

Address:

Telephone number:

Email address:

RETURNING YOUR COMPLETED FORM:

Please send your completed form (with proof of identity) to:
Cooperative Learning Institute Limited
41 Marley Court, Rathfarnham, Dublin 14, D14 E048.

FOR COMPANY USE ONLY:

Reference No:	DP/
Date request received:	
Identity verified:	YES/NO
If yes: Original ID supplied in person?	YES/NO
If yes, ID checked and returned to requester?	YES/NO
Copy ID attached to request:	YES/NO
If yes, ID verified and documents shredded by:	

Privacy Notice for the Data Subject Access Request

The purposes for which The Cooperative Learning Institute Limited processes your data are:

- To verify your identity;
- To verify your address;
- To establish if you are an adult or a child;
- To identify the personal data for which you have requested a copy;

Legal basis:

- Article 12 of the General Data Protection Regulation;
- In the event that you do not provide the information requested on this form it may not be possible to provide a copy of the data requested;

Categories of data subject:

- Requester of data Categories of personal data;
- Identity including any reference numbers provided;
- Address and other contact details;
- Details of their contacts with the Department where relevant to their request;

Recipients of the data

- The data provided may be shared with the Data Protection Commissioner where requested by that office;

Storage period

- The data processed will be retained for a period of 3 years and subject to review thereafter;

Third Country

- None of your data will be transferred to a country outside of the European Economic Area i.e. the EU and Norway, Iceland and Liechtenstein;

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Contact Details

- The Cooperative Learning Institute Limited is the data controller for the processing of your data. If you have any query in respect of this you may contact the Director or by post to Cooperative Learning Institute Limited, 41 Marley Court, Rathfarnham, Dublin 14, D14 E048.

Appendix 2: Website Privacy Notice

This Privacy Notice governs the manner in which The Cooperative Learning Institute Limited collects, uses, maintains and discloses information collected from users (each, a "User") on the website ("Site"). This Privacy Notice applies to the website and our organisation.

Data Controller:

Cooperative Learning Institute Limited
41 Marley Court,
Rathfarnham,
Dublin 14,
D14 E048.

Personal Data (in connection with the provision of services to our school clients):

We use personal data in a variety of ways in connection with the delivery of services to schools. We process this data in most cases, as per our contractual obligation to the school.

- Student's Data includes First Name, Surname & Class;
- Teaching Staff includes First Name, Surname Email Address & Class;

How we use collected information (including data processes in connection with the provision of services to our school clients):

We use personal data for purposes including:

- provision of training and support to the school;
- provision of our proprietary sociometric tool to the school;
- to comply with our contractual obligations with the school;
- to promote our legitimate business interests;
- to comply with our legal obligations as limited company;
- to comply with our reporting obligations to various government bodies i.e. CRO, Revenue;
- to provide appropriate training, direction and support to our staff;

How we protect your information:

We adopt appropriate data collection, storage, processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We keep your personal information for a length of time as per our Retention Policy i.e. For our software client's data, this generally means we will retain data for up to 30 days after your contract of service expires. After this time, your data will be destroyed by shredding or anonymization on our database. In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in our Data Protection Policy.

Sharing your personal data:

From time to time, we may share personal data (arising out of the provision of services or our own company data) with An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc. The sharing of personal data and the nature of what is shared depends on various factors. We may also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed. At all times, we shall ensure that the sharing of information is done so as per the requirements of the GDPR.

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent;
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this Statement please contact us below.

Personal Identifiable Information (Website)

We may collect personal identification information from users in a variety of ways in connection with activities, services, features or resources we make available on our Site. We will collect personal identification information from Users only if they voluntarily submit such information to us. Users can always refuse to supply personally identification information, except that it may prevent them from engaging in certain Site related activities.

Non-personal Identifiable Information (Website)

We may collect non-personal identification information about users whenever they interact with our Site. Non-personal identification information may include the browser name, the type of computer and technical information about Users means of connection to our Site, such as the operating system and the Internet service providers utilized and other similar information.

Our use of cookies

Cookies are small pieces of code sent from websites to your device and used to store information by your web browser (see <http://www.youronlinechoices.com/ie/>). Our use of cookies and other technologies may collect information such as your IP address, operating system, the browser you use and the frequency and length of your visits to our website. This information is treated as your personal information by The Cooperative Learning Institute Limited under the terms of this Statement.

We use cookies and other technologies to:

- keep track of how you interact with our website;
- target advertising;
- keep track of how you access and download our materials; and
- offer functionality on our website, including social media plug-ins and sharing.

Changes to this privacy policy

The Cooperative Learning Institute Limited may from time to time update this privacy policy. We encourage Users to frequently check this page for any changes to stay informed about how we are helping to protect the personal information we collect. You acknowledge and agree that it is your responsibility to review this privacy policy periodically and become aware of modifications.

Links

Some pages of our Website include external links to third party websites. We have no control over and are not responsible for these websites or the use of your information by third parties. You should check the privacy notices on any third party websites to ensure that you are satisfied with their privacy practices, prior to sharing any personal information.

Appendix 3: Staff Privacy Notice

Data Controller:

Cooperative Learning Institute Limited
41 Marley Court,
Rathfarnham,
Dublin 14,
D14 E048.

This Privacy Notice governs the manner in which Cooperative Learning Institute Limited collects, uses, maintains and discloses information collected throughout the recruitment, hiring and employment of staff.

Personal Data

We collect personal identification information from staff and prospective staff in a variety of ways in connection with your employment at the Cooperative Learning Institute Limited.

Staff / Recruitment Data (Lawful Basis: Public Interest, Contractual Obligation, Legal Obligation):

- Name, Address, Date of Birth, Phone Number;
- PPSN;
- Vetting No.;
- Payment details;
- Statutory deductions Voluntary deductions;
- Service history;
- Leave including Sick leave / Secondments;
- Qualifications & Results (2nd & 3rd Level) & Work Experience;
- Particulars of your cases where you may query the application of the terms and conditions e.g. Contract of indefinite duration;

How we use collected information

We use your personal data for purposes including:

- your application for employment;
- to provide you with appropriate direction and support in your employment;
- to care for your health and well-being;
- to coordinate, evaluate, fund and organise educational programmes;
- to comply with our legal obligations as an employer;
- to process appeals, resolve disputes, and defend litigation etc.

How we protect your information

We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We keep your personal information for a length of time as per our Retention Policy i.e. For staff we will retain data for the duration of employment and up to 7 years thereafter. After this time, your data will be destroyed by confidential shredding or deletion from our database.

In certain circumstances we may retain your data longer, these circumstances and the retention period are outlined in the Cooperative Learning Institute Limited Data Protection Policy.

Sharing your personal information

From time to time, we may share personal data (arising out of the provision of services or our own company data) with An Garda Síochána, HSE, the Department of Social Protection, our Insurance Company, the Revenue Commissioners etc. The sharing of personal data and the nature of what is shared depends on various factors. We may also share personal data with other third parties including our insurance company and other service providers (including IT providers, security providers, legal advisors etc.) as needed. At all times, we shall ensure that the sharing of information is done so as per the requirements of the GDPR.

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this statement please contact us.

Appendix 4: The Cooperative Learning Institute Limited Email Privacy Notice (for inclusion in all email signatures)

Example (in bold below for effect):

Best regards,

Director
Cooperative Learning Institute Limited
41 Marley Court,
Rathfarnham,
Dublin 14,
D14 E048.

This email and any files transmitted with it are confidential and intended solely for the use of the individual or entity to whom they are addressed. If you have received this email in error please notify the sender. This message contains confidential information and is intended only for the individual named. If you are not the named addressee you should not disseminate, distribute or copy this e-mail.

DATA PROTECTION: We're processing data belonging to you i.e. your email address & name in the Public Interest. For more information please review our Privacy Notice [here](#).

Appendix 5: Training Course Privacy Notice

Data Controller:

Cooperative Learning Institute Limited
41 Marley Court,
Rathfarnham,
Dublin 14,
D14 E048.

This Privacy Notice governs the manner in which The Cooperative Learning Institute Limited collects, uses, maintains and discloses information collected throughout our training programmes.

Personal Data:

We use personal data originating from training courses in a variety of ways. We process this data in most cases, as per our contractual obligation to the school.

- Name, Address, Date of Birth, Phone Number, Place of Employment (School);

How we use collected information:

We use your personal data for purposes including:

- to provide appropriate training, direction and support to attendees at our training programmes;
- to communicate with you following successful completion of the course;

How we protect your information:

We adopt appropriate data collection, storage and processing practices and security measures to protect against unauthorized access, alteration, disclosure or destruction of your personal information.

How long do we keep your personal information?

We will permanently archive your data 2 years after the course takes place.

Sharing your personal information

We do not sell or trade personal data to others. We will share your certification with your (place of employment).

Your rights

You have a number of rights in relation to your personal information. These rights include the right to:

- request information regarding the personal data that we hold about you and the source(s) of that information. You can request a copy of any personal data we hold about you. This service is free of charge.
- request that we rectify without undue delay any inaccuracies in relation to the personal data we hold;
- in some circumstances, request the erasure of your personal data or object to the processing of your data;
- obtain restriction of processing in some circumstances;
- object to any processing in some circumstances;
- in some circumstances, request that your personal data be transferred to you or a new school if the data is processed automatically (Please note, that we retain only a copy of certain data collected from you. Furthermore we do not avail of systems that make automated decisions based on your data);
- if we are processing any data for which you have given consent, you may withdraw consent to us processing your personal data. This will not affect the processing already carried out with your consent; and
- lodge a complaint with a supervisory authority. In Ireland, this is the Office of the Data Protection Commissioner;

Any enquiries regarding the above rights or if you wish to exercise any of these rights or any other rights provided for in this statement please contact us.

