z

DATA PROTECTION POLICY

General Data Protection Act (GDPR)
Updated 2024

Contents

Appendices

Introduction

The purpose of this document is to provide a concise policy statement regarding the Data Protection obligations of Sligo Social Service Council CLG. This includes obligations in dealing with personal data, in order to ensure that the organisation complies with the requirements of the relevant Irish legislation, namely the Irish Data Protection Act (1988), the Irish Data Protection (Amendment) Act (2003), and the General Data Protection Regulation (GDPR) (2018).

Rationale

Sligo Social Services must comply with the Data Protection principles set out in the relevant legislation. This Policy applies to all Personal Data collected, processed and stored by Sligo Social Services in relation to its staff, service providers and clients in the course of its activities. Sligo Social Services makes no distinction between the rights of Data Subjects who are employees, and those who are not. All are treated equally under this Policy.

Purpose of this policy

The purpose of this Policy statement is to protect the rights and privacy of individuals in accordance with the Data Protection Act (1988), the Data Protection (Amendment) Act (2003) and the General Data Protection Regulation (GDPR) (2018). This applies to records of all types regardless of the medium on which they are held.

Scope

The Policy covers both personal data and special categories of personal data held in relation to Data Subjects by Sligo Social Services. The policy applies equally to personal data held in manual and automated form. All personal data and special categories of personal data will be treated with equal care by Sligo Social Services. Both categories will be equally referred to as Personal Data in this policy, unless specifically stated otherwise.

Principles relating to processing of personal data

Sligo Social Services undertakes to perform its responsibilities under the legislation in accordance with the seven principles contained in Article 5 of the act, which will regulate the processing of personal data.

Personal data shall be:

a) **Lawful, fair and transparent processing** – Sligo Social Services processes personal data based on lawful processing conditions. The Data Subject should have full and transparent knowledge of the identity of the parties to the processing, the purposes of the processing, the recipients of personal data, the existence of Data Subject rights and freedoms, and how to contact the Controller.

b) **Specified and lawful purpose** – personal data will be processed only for a specified purpose. For example, data which is collected for the purpose of a newsletter cannot automatically be used to target the Data Subject with regular fundraising campaigns.

c) **Minimisation of processing** – processing of personal data will be adequate, relevant and restricted to what is necessary in relation to the purposes for which they are processed. Not only will this relieve the organisation of the burden of performing actions on personal data, which are not required or necessary, but it will also reduce the overall risk of data breaches. For example, where a non-profit organisation wishes to ensure that the Data Subject is not a child, it may not be necessary to collect the date of birth of the Data Subject. A year of birth can be provided or the Data Subject can simply confirm at registration that he or she is over the legitimate age.

d) **Accuracy** – personal data shall be accurate and where necessary kept up to date. Sligo Social Services must rectify any incorrect data and erase any data, which is known to be erroneous or obsolete.

e) **Storage limitations** – Personal data shall be kept in a form which permits the identification of Data Subjects for no longer than is necessary for the purposes for which the personal data is processed. *See Data Retention and Destruction Procedure Appendix 1.*

f) **Security and confidentiality** – Sligo Social Services will employ high standards of security in order to protect the personal data under its care. Sligo Social Services Password Policy, Data Sharing and Confidentiality Agreement and Data Retention and Destruction Procedures guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Sligo Social Services in its capacity as Data Controller. Access to and management of staff and client records is limited to those staff members who have appropriate authorisation and password access. Sligo Social Services will carry out regular internal security audits.

g) **Liability and accountability** – The Data Controller and the Data Processor will comply with the General Data Protection Regulations (GDPR). The Data Controller will exercise reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR.

Roles and Responsibilities

Line Managers/Supervisors are responsible for:

- The implementation of this policy and all other relevant Sligo Social Services policies within the services/areas for which they are responsible
- Ensuring that all Sligo Social Services employees who report to them are made aware of and are instructed to comply with this policy and all other related Sligo Social Services policies
- Consulting with the Data Controller in relation to the appropriate procedures to follow when a breach of this policy has occurred.
- Each Manager is responsible for ensuring that the organisation and those processing data (employees and external Data Processors), conducts itself appropriately in compliance with GDPR.
- The manager will conduct regular audits of their service to ensure that Sligo Social Services as a Controller meets it obligations with regard to data protection legislation.
- The manager should acquire a knowledge of data protection law and practices.
- The manager will be involved in all data protection issues for their specific area as early as possible.

All Staff are responsible for:

- Complying with the terms of this policy and all other relevant Sligo Social Services policies, procedures, regulations and applicable legislation
- Respecting and protecting the privacy and confidentiality of the information they process at all times
- Reporting all misuse and breaches of this policy to their line manager

Sligo Social Services as a Data Controller

Sligo Social Services processes a multiplicity of data including but not restricted to; client files, HR records, financial records, company records and general administrative records. The organisation is committed to ensuring that all staff have sufficient awareness of the GDPR requirements in order to be able to anticipate and identify a Data Protection issue, should one arise. In such circumstances, staff must ensure that the appropriate manager is informed, in order that appropriate corrective action is taken.

There is a regular and active exchange of personal data between Sligo Social Services and the individuals on whom data is held. This Policy provides guidelines for the exchange of information, as well as the procedure to follow in the event that a staff member is unsure whether such data can be disclosed. In general terms, the staff member should consult with their manager to seek clarification.

Data Processor

The Data Processor is any person or organisation who processes data on behalf of Sligo Social Services e.g. IT Company, pension providers, any company with remote access to Sligo Social Services computers. Article 28 of the Act states that the Data Processor can only process data under instruction from the Data Controller and the Data Processor has committed themselves to confidentiality. The Data Processor will

assist Sligo Social Services with regards to Data Protection Impact Assessments and Data Breach compliance. On end of service contract, the Data Processor must return all data to Sligo Social Services. The Data Processor must make available to Sligo Social Services all information necessary to demonstrate compliance with GDPR.

Sligo Social Services and Data Processor Relationship

Sligo Social Services will only use Data Processors that will provide sufficient guarantees to implement appropriate measures that ensures compliance and protection of the rights of the individual. The Data Processor will not engage another Processor (Sub Processor) without prior specific or general written authorisation from Sligo Social Services. Sligo Social Services will have an agreement detailing the contract in place binding the Data Processor. The agreement will set subject matter and duration of processing, purpose of processing, type of personal data, and the obligation and rights of Sligo Social Services as the Controller. If a Sub Processor fails to fulfil its data protection obligations, the primary processor shall remain fully liable to Sligo Social Services for the performance of the Sub Processor's obligations. *See Data Processing Agreement Appendix 1*

Collecting Information

Individuals on whom we hold personal data should be advised that we will collect information from them which will be recorded on a file. They will be advised of the types of medium used to store this data. Individuals will be told that all staff in Sligo Social Services have a duty of confidentiality and there are strict rules about who will have access to the record. An individual's personal information will not be shared with any other person or organisation without the individual's knowledge and permission, unless there is a legal requirement, if there is a child or adult safeguarding issue, or a perceived risk of harm. A breach of confidentiality is when a person shares information with another in circumstances where it is reasonable to expect that the information will be kept confidential. *See Data Sharing and usage agreement Appendix 2*
All information will be held in accordance with the seven principles contained in Article 5 of the act.
Sligo Social Services will:

- Ensure that individuals are made aware of the right to be informed that information is collected, who is collecting it and the purpose for which it is collected.
- Ensure that an individual's explicit consent, written or verbal, is obtained prior to recording and holding information. In the case of children and young persons, an adult parent or guardian can give consent on behalf of the child.
- Ensure that the individual knows the identity of the Data Controller
- Furnish the individual with contact details of the manager for that specific area
- Let the individual know if and who you will be sharing data with

- Ensure that the individual knows about data retention duration *See Appendix 2, Data Retention Periods*
- Ensure that individuals are informed of their rights to access personal data held by Sligo Social Services.
- Ensure that individuals are advised of their right to make a complaint to the Data Protection Commissioner if they are unhappy with how Sligo Social Services is discharging its duties under the Act.

See Sample Privacy Notice Appendix 3

Consent

Individuals must give consent for Sligo Social Services to process personal data and Sligo Social Services must demonstrate that the individual has consented to processing personal data. Consent must be freely given and must be an unambiguous indication of the individual's wishes. An individual has the right to reverse the decision of consent if they so wish. Where possible written consent should be sought. Manner in which consent is received will be recorded in the individual's file whether manual or automated. *See appendix 4, Information and Consent Form*.

Consent relating to Children

Under Irish law a child is defined as a person under the age of 18 years (Children's Act 2001). When a person is under 18 years, consent is given or authorised by the holder of parental responsibility over the child (Parent/Guardian).

Subject Access Request

Sligo Social Services will allow the individual right of access to their personal data which was collected concerning him or her. The individual must make a request in writing and the Sligo Social Services Data Controller will respond to the request within 30 days. The individual has the right to request from Sligo Social Services:

- Confirmation of processing of data relating to Data Subject
- Where such personal data are being processed
- Access to the data held
- Purposes of the processing
- Categories of personal data concerned
- Discloses recipients to whom the personal data has been or will be disclosed.

- Where possible, the envisaged period for which the personal data will be stored and criteria used in determining storage duration.
- Notification obligation, if dissatisfied with response the individual can go to the Data Protection Commissioner. The individual must be notified that they can do this in response. *See Subject Access Request Form Appendix 5*

Data Breaches

A Data Breach is the intentional or unintentional release of secure information to a person/company/other body who should not have access to this information. This can likely result in the risk to the rights and freedoms of individuals due to; identity theft, social engineering, fraud, financial loss. Sligo Social Services staff who have access to personal data or are involved in the processing of personal data will ensure that appropriate security measures are taken against unauthorised access to or unauthorised alteration, disclosure or destruction of data, in particular where the process involves transmission of data over a network.

Do Not:

- Use external storage devices i.e. USB memory sticks to store or transfer personal data.
- Store personal data on any laptop or mobile device that is not encrypted
- Divulge or set weak passwords *see Password Procedures appendix 8*
- When emailing multiple recipients reveal their email addresses. Use Bcc in email address bar.
- Open or reply to suspicious emails
- Use a computer that does not have up-to-date anti-virus software
- Allow remote computer access to any unauthorised person
- Leave filing cabinets unlocked
- Leave personal data where it can be viewed by others
- Use public Wi-Fi to process personal data

Data Breach Notification

Actual, suspected or potential breaches will be reported immediately to the manager. Any employee who becomes aware of a likely data breach and fails to notify the manager will be subject to Sligo Social Services disciplinary procedures.

If a breach occurs, Sligo Social Services will communicate to the individual a personal data breach without delay, especially where that personal data breach is likely to result in a high risk to the rights and freedoms of the individual, in order to allow him or her to take the necessary precautions. The communication should

describe the nature of the personal data breach as well as recommendations for the individual concerned to mitigate potential adverse effects. Such communication to individuals will be made as soon as reasonably feasible and in close co-operation with the supervisory authority (Office of the Data Protection Commissioner, Dublin) if the breach is considered high risk.

Sligo Social Services and Data Processors must report data breach within 72 hours of becoming aware of data breach to Supervisory Authority. The following details must be provided:

- Details of the breach and number of data subjects affected
- Details of manager of that specific area or other appointed contact
- Impact of breach
- Containment and mitigation measures

Sligo Social Services must keep a record of data breach as proof of compliance

- Must be produced on request by supervisory authority
- Maintain a breach log and review regularly

Notification may not be required if:

- Data is already encrypted
- Technical safety measures are in place
- Doing so would involve disproportionate effort

Where devices or equipment containing personal data are lost or stolen, the Supervisory Authority is only notified if data on such devices is not encrypted.

Recording Data Breaches

All data breaches will be recorded in the Data Breaches Register, which is kept by the Data Controller or someone appointed by the Data Controller. The register will contain 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 will include a description of the incident, was the individual informed, if not, why not. Was the Supervisory Authority informed, if not why not. Such records will be provided to the Supervisory Authority upon request. *See Personal Data Breach Report Form Appendix 6*

Data Protection Impact Assessment (DPIA)

When doing a DPIA you must describe the processing, assess the necessity and proportionality of a processing and manage the risks to the rights and freedoms of natural persons resulting from the processing of personal data (by assessing them and determining the measures to address them). The DPIA is an important tool for accountability and will help Sligo Social Services comply with requirements of the GDPR. The DPIA will also demonstrate that appropriate measures have been taken to ensure compliance with the Regulation. Under the GDPR, non-compliance with DPIA requirements can lead to fines imposed by the competent supervisory authority. Failure to carry out a DPIA when the processing is subject to a DPIA, carrying out a DPIA in an incorrect way or failing to consult the competent supervisory authority where required, can each result in an administrative fine of up to 10M€, or in the case of an undertaking, up to 2% of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The GDPR does not require a DPIA to be carried out for every case, it is only mandatory where a processing is "likely to result in a high risk to the rights and freedoms of natural persons".

Records	Risk	Containment and Mitigation Measures	Result
Client records non child protection, Client records child protection, HR records, Financial records, Company records,	• Release of Personal or sensitive personal information to an untrusted environment • Identity theft • Social Engineering • Fraud • Financial Loss • Destruction of personal data	• Encryption • Password Protection • Limited access • Physical security i.e. locked filing cabinets, offices etc. • Regular audits on security practices • Competent careful staff • Contracts with third parties • Report breaches immediately	Reduced risk to the rights and freedoms of Data Subjects

General admin records.	• Alteration of personal data Loss to reputation and • trust	• • Pseudonymisation were possible Storing data for no longer than is • necessary Complete compliance with GDPR • Safe destruction of data	

Audit for Compliance

The Manager of each service will conduct regular audits (not less than twice a year) to ensure that Sligo Social Services as a Controller meets it obligations with regard to data protection legislation. They are responsible for ensuring that the organisation and those processing data on behalf of the organisation acts or conducts itself appropriately in compliance with legislation. The Manager must keep a log of audits conducted. Here is a useful checklist:

Service Area _____

Date of Audit_____/_____/_____

Physical security checked – you may consider when checking physical security:

◯ Are filing cabinets locked?
◯ Are keys securely stored?
◯ Are rooms locked when not in use?

Automated file security checked – you may consider when checking automated file security:

◯ Are passwords used in line with Password Protection Policy?
◯ Are computers encrypted?
◯ Is remote access being monitored?
◯ Are agreements in place with Data Processors?
◯ Are outside Data Processers compliant with GDPR?
◯ Are files kept up-to-date?
◯ Are files easily accessible should there be a Subject Access Request?
◯ Are files kept only for the length of time stated in the File Retention Procedure?
◯ Are files destroyed under confidential conditions and in line with File Destruction Procedure?

Manual file security checked – you may consider when checking manual file security:

◯ Can personal data be accessed by unauthorised persons?
◯ Are files left lying around?
◯ Are print-outs retrieved immediately from the printer or photocopier?
◯ Are files kept up-to-date?
◯ Are files correctly labelled?
◯ Are files kept only for the length of time stated in the File Retention Procedure?

Signed by Manager: _____

Data Retention and Destruction

This document is intended to be read along with the Data Protection Policy.

All staff responsible for the retention of records are also responsible for the proper destruction of records following the stated retention period.

Sligo Social Services is committed to effective records management retention and disposal to ensure that it:

- Meets legal standards in terms of retention periods
- Optimises the use of space
- Minimises the cost of record retention
- Securely destroys outdated records

This procedure applies to all official records generated in the course of Sligo Social Services operations, including but not limited to:

- Typed, or printed hardcopy, manual (i.e., paper) documents;
- Electronic records and documents (e.g., email, web files, text files, PDF files);
- Video or digital images;
- Graphic representations;
- Records on storage devices or any electronic devices;
- Electronically stored information contained on network servers and/or document management systems; and
- Recorded audio material (e.g., voicemail).

Manual records must be destroyed by shredding or other means to ensure that all sensitive or confidential material can no longer be read or interpreted. All electronic records must be deleted from the device in which they are held, copies to the server and the cloud will also be deleted.

Definition of Records

A record is defined under the Freedom of Information Act 1997 and 2003 as "any memorandum, book, plan, map, drawing, diagram, pictorial or graphic images or both, any form in which data (within the meaning of the Data Protection Acts 1988, the amended act 2003, and the General Data Protection Regulation (GDPR) 2018) are held, any other form (including machine-readable form) or device in which information is held or stored manually, mechanically or electronically and anything that is a part copy, in any form of any of the foregoing or is a combination of two or more of the foregoing" (Freedom of Information Act 1997, 2003).

Records created by Sligo Social Services should be both accurate and complete. They must provide evidence of the function or activity they were created to document. In order to be evidential, records must be authentic, reliable, have integrity and be useable.

An authentic record is one that can be proven to be what it purports to be. In order to ensure that the records created are authentic then records should be dated, timed and signed. They should be placed into the filing system to form part of the retention schedule so that they are protected against unauthorised addition, deletion or alteration.

A reliable record is one that can be trusted to be an accurate representation of a function. Therefore, records should contain all relevant facts and be created at the time of the action or transaction or as soon as possible afterwards by a person authorised to carry out that function, action or transaction.

The integrity of a record refers to it being complete and unaltered. Once created, additions or annotations to the record can only be carried out by those authorised to do so and any amendment should be explicitly indicated on the record.

A useable record is one that can be located, retrieved, presented and interpreted or read whenever or wherever there is a justified need for that information. It should be traceable within a records management system. Record schedules and filing indices that capture the records are essential in ensuring records are useable.

In electronic records, contextual information is required in addition to the physical transfer of records to ensure their continued usability.

Records retained will be original (or an electronic copy, transferred using the appropriate and verifiable system) unique or of continuing importance to Sligo Social Services.

Record Retention Periods

Sligo Social Services will comply with the Data Protection Acts 1988, the amended act 2003, and the General Data Protection Regulation (GDPR) 2018. The Acts set out the principle that personal data shall not be kept for longer than is necessary for the purpose or purposes for which it was obtained.

This requirement places a responsibility on Sligo Social Services to be clear about the length of time personal data will be kept and the reasons why the information is being retained.

This document is in compliance with those provisions and includes defined retention periods for records and systematic disposal of records within a reasonable period after the retention period expires. Since 2003, Data Protection Legislation applies to both electronic and hard copy records. *See Data Retention Appendix 7*

Manual and Electronic Files

Sligo Social Services creates files in manual form for many of our service users. Once the client is no longer using the service or reasonably expected to return to avail of the service the clients file will be closed. From 2018 onwards the files will be retained in a manual electronic form, and stored centrally. Once stored electronically the paper copy of these files will be destroyed as per confidential shredding procedure. Files closed prior to 2018 will be retained in paper form and stored centrally pending year of destruction.

From 2018 onwards it is the responsibility of Managers to ensure that closed files are scanned, retained and destroyed as per the Data Retention Periods procedure. The Manager of each service will keep a log of every manual record that has been closed, sent to Admin and scanned into the centralised folder, giving instructions regarding retention periods. This will allow managers to track files, intended retention periods, and whether or not a file was destroyed or held in perpetuity.

Closing a File

When a manual file is closed, the manager will fill out the *File Storage and Destruction forms Appendices 8 and 9*.

File ID Numbers

File ID numbers will be generated by the manager for each service. Each ID number will start with the code for that specific area followed by 0001, 0002, 0003, and so on. Codes will be created centrally by Administration while number can be done locally and should be sequentially.

Example: The first file closed and ready for scanning from the meals on wheels service will have the ID MOW0001.

The Administrator will then carefully scan all documents into the centralised folder which will contain folders for each service. When the administrator is satisfied that the file has been scanned correctly, the original manual file will be shredded under confidential conditions. Each service folder will contain folders for each year in which the files will be destroyed. Each year of destruction folder will contain the individuals file e.g. joebloggsMOW0001 and the entire scanned hard copy of the individuals file.

Retrieving Files from Centralised Folder

Where a file has been closed, scanned into the Centralised Folder and the client returns to the service the manager must request for the file in writing to the Administration. The file will be provided in paper form to the Manager. The Administrator will then delete the file from the centralised electronic folder, recycle bin, server and subsequently the cloud. The Administrator will not list the deletion of the electronic manual file in the Destruction Register as the file still exists in paper format. Upon the individual leaving the service again, the manager will follow the same steps for closing a file.

Reporting of Irregularities

Any member of staff who considers that there may have been an irregularity in the records management or destruction process must inform the manager immediately.

If you have questions about the retention or destruction of specific documents or the data types they contain. Please contact your manager.

File Destruction

After a file has been held in the Centralised Folder for the appropriate length of time as per the Data Retention Periods procedure, the Manager will instruct the administrator to destroy the file by sending an explicit email to the administrator who manages the Centralised File. In the email, the manager will list the following information:

- Date record will be destroyed
- What service the record belongs to
- Individuals Name and ID
- Individuals Date of Birth
- Name of manager who is authorising destruction

The administrator will enter the above details into the *Destruction Register* and attach email from manager to the Destruction Register. The administrator will then remove the Data Subjects file from the Centralised folder by:

- Deleting Data Subject's file
- Emptying the recycling bin
- Removing file from Server

Note: After file has been removed from the server, it will remain in the cloud for 30 days, then it will automatically be deleted. After 30 days the Data Subject's file cannot be retrieved.

If an individual wants their file destroyed upon leaving the service, the individual does have the "right to be forgotten" if the data processing is no longer necessary as purposes are no longer relevant. The individual can withdraw consent or object to processing at any time unless the data refers to information in relation to child abuse, a child in foster care or an action under 'Safeguarding Vulnerable Adults Policy'

Data Retention Schedule

The Data Protection Act recognises that different categories of data can reasonably be retained for different periods of time. The length of time different categories of personal data are retained for is based on the following:

- The current and future value of the information
- The cost, risks and liabilities associated with retaining the information
- The ease or difficulty of making sure it remains accurate and up to date

Low Risk e.g. general admin files which have a lower retention period.

Medium risk files relating to staff, or adult clients without Child Protection Issues or disclosures of elder abuse are kept for the current year plus 7 years after file closed.

High Risk files are any files relating to Child Protection issues, children in foster care, an action taken under 'Safeguarding Vulnerable Adults Policy', or any issue relating to elder abuse. High risk files are kept in perpetuity.

Suspension of Record Disposal in Event of Litigation or Claims

In the event any employee of Sligo Social Services reasonably anticipates or becomes aware of an audit or the commencement of any litigation against or concerning Sligo Social Services, such employee shall inform their Manager and any further disposal of documents shall be suspended until such time as the Manager, with the advice of the CEO, determines otherwise. The Manager shall take such steps as are necessary to promptly inform affected staff of any suspension in the disposal or destruction of documents.

All paper documents destroyed pursuant to this Policy shall be cross-cut by mechanical shredder by a person appointed by Sligo Social Services. Electronic data contained on servers and hard drives shall be deleted and overwritten also by a person appointed by Sligo Social Services. Electronic data contained on all other media shall be destroyed by the physical destruction of that media.

Manual Records Destruction Process

It is the individual responsibility of all staff to ensure information they are handling is destroyed effectively, securely and in accordance with this regulation. Manual records that have reached the end of their lifecycle, either in accordance with the relevant Records Retention Schedule or as usual paper waste, are divided into two categories, and are destroyed in accordance with the instructions relating to each category.

1. Paper Recycle Bins
   For non-confidential records and/or data, and those containing no personal information, bins are provided for recycling purposes. All recycle bins are emptied whenever necessary by facilities staff. As paper collected in the bins is only ever recycled and never shredded, it is the responsibility of all those placing material in the bins to check that it has been identified correctly for recycling.

2. Shredding
   Any record containing the data described below is treated as highly confidential material.
   - Data relating to confidential financial activities of Sligo Social Services
   - Payroll and pension data
   - Sensitive personal data, as defined by the Data Protection Act, 1988, 2003, and the General Data Protection Regulation 2018 covering racial or ethnic origin, political opinions, religious beliefs, Trade Union activities, physical or mental health, sexual life, or details of criminal offences
   - Higher level personal data, such as information relating to staff disciplinary proceedings or harassment
   - Records containing "private" personal data, such as information relating to an individual's personal circumstances, personal finances, or a personal reference
   - Records of a commercially sensitive nature, such as contracts, tenders, purchasing or legal documents
   - Records concerning intellectual property rights, such as unpublished research data, draft papers, and manuscripts
   - Records containing personal or sensitive data about research subjects.

A "confidential" record will be shredded confidentially by a designated member of staff. The date of destruction and the manner in which the records are destroyed will also be recorded. In terms of the means of destruction this will be carried out by shredding.

Contractors used to carry out any of the aforementioned processes will be required to sign confidentiality undertakings and to produce written certification as proof of destruction. To ensure a higher level of security, it is recommended that a nominated staff member should be present during both the transportation and records destruction process.

Electronic Records Destruction Process

Electronic records containing confidential information require a two-step process for assured, confidential destruction. Deletion of the contents of digital files and emptying of the desktop "trash" or "waste basket" is the first step. It must be kept in mind that restoration of "deleted" files is possible in the hands of

computer specialists. With regard to records stored on a “server” and backed up to the “cloud”, data is encrypted before it is sent to the cloud and is then stored in an encrypted format. This data cannot be accessed without the encryption key. Once the data has been deleted from the desktop and then the server, files will be retained in the cloud for no longer than 30 days, then the data will automatically be deleted. With regard to external back-up drives and memory sticks, it is recommended that these storage devices be physically destroyed.

Holding a File in Perpetuity

When a file is to be retained in perpetuity, the manager will follow the same steps for closing a file. In the *File Storage and Retention form,* the manager will clearly state that the file is to be held in perpetuity by ticking yes under hold in perpetuity. The administrator will then carefully scan all documents into the Centralised Folder, then into the correct service folder, and finally the folder marked perpetuity. When the Administrator is satisfied that the file has been scanned correctly, the original manual file will be shredded under confidential conditions.

Cookies Policy

Sligo Social Services Council CLG

Last update: October 2020

What is a Cookie?

A cookie is a small piece of data in the form of a text file that may be stored on your computer or mobile device having visited a website. It allows a website “remember” your actions or preferences over a length of time.

How are Cookies Used?

There are two main categories of cookie

Session Cookies: These temporary cookies are not stored on your computer or mobile device. They are erased once your browser is closed out or your session is inactive for 20 minutes or more.

Persistent cookies: Persistent or Duration cookies are placed on your computer or mobile device for a pre-determined duration once you visit a website.

Sligo Social Services does not use cookies on its website. However, Sligo Social Services have a live link to the Sligo Social Services Facebook page and Facebook uses the following Cookies:

Cookie	Description	Duration	Type
Fr	The cookie is set by Facebook to show relevant advertisements to the users and measure and improve the advertisements. The cookie also tracks the behaviour of the user across the web on sites that have Facebook pixel or Facebook social plugin.	2 months	Advertisement
Sb	This cookie is used by Facebook to enable its functionalities.	2 years	Functional
Wd	The cookie is set by Facebook or Facebook social plugins to measure and store the dimensions of the browser window. This cookie is used by	1 week	Advertisement

	Facebook to optimize the rendering of the page.		
Datr	This cookie is set by Facebook for the purpose to identify suspicious login activities, fake and spammy accounts, keep users account and their content safe, and to prevent Distributed Denial of Service.		

In order to be compliant with data protection, Sligo Social Services have implemented a cookie management plug-in.
Please follow the link below to view Facebook's Cookies Policy
https://www.facebook.com/policies/cookies/

Passwords

1.0 Overview

Strong passwords are critical to computer security. They are the first line of defence for user accounts. A poorly chosen password which is easy to guess, or one left in open view could cause the entire network to be compromised or may result in unauthorised access and / or exploitation of Sligo Social Service files.

All staff, including IT contractors or vendors with access to Sligo Social Services systems, are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this procedure is to present best practice for the creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this procedure includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Sligo Social Services facility, has access to Sligo Social Services network, or stores any non-public Sligo Social Services information.

4.0 Procedure 4.1 General

Users must note that passwords are for their own personal use and must not be shared or disclosed to anyone. It is an offence under the Computer Misuse Act 1990 to access or attempt to gain access to a computer system or computer material to which one is not entitled.

In addition, it is a breach of this policy for any staff to misuse their own or other user's password. If any such misuse results in a staff knowingly elevating their system privileges above those that they have been authorised to use then this will be considered an act of gross misconduct.

- Remote access to privileged accounts (e.g. root, enable, windows admin, application administration accounts, etc.) must not be attempted from insecure locations e.g. open access cluster systems or public terminals.
- All system – level passwords (e.g. root, enable, windows admin, application administration accounts, etc.) must be changed on at least an annual basis by the I.T. Administrator or Sligo Social Services Third Party IT Company.
- All user-level passwords (e.g. email, web. Desktop computer etc.) must be changed at least annually by the I.T. Administrator.
- User accounts that have system-level privileges granted through group memberships or programmes such as "the X Drive, Internet banking portals" must have unique passwords from all other accounts held by that user.
- Passwords must not be inserted into email messages or other forms of electronic communication.
- All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General password construction guidelines

All members of staff in Sligo Social Services should be aware of how to select strong passwords.

Strong passwords have the following characteristics:
Contain at least three of the five following character classes:

1. Lower case characters
2. Upper case characters
3. Numbers
4. Punctuation
5. "Special" characters (e.g. @ # $ % & + () -1 ~ = ^ ¬|/etc.) Contain at least thirteen alphanumeric characters.

Weak passwords have the following characteristics:

- If the password contains less than thirteen characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as: ○ Names of family, child(ren), car, hometown, favourite food, favourite car or sports club, pets, friends, co-workers, fantasy characters, etc.
- Computer terms and names, commands, sites, companies, hardware, software.
- The words "Social Services", "sligo", "social" or any derivation
- Birthdays and other personal information such as addresses and phone numbers
- Words or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc. • Any of the above spelled backwards
- Any of the above preceded or followed by a digit (e.g. secret1, 1secret)

Try to create passwords that can be easily remembered. One way to do this is to create a password based on a song title, affirmation, or other phrase, e.g., the phrase might be; "this may be one way to remember" and password could be "Tmb1w2R! or "TMB1wr~" or some other variations.

Do not use either of these examples as passwords!

If you're unsure about whether your password is good enough, run it through Microsoft's free password checker. ***Never use a password rated less than "Strong"***

B. Password Protection Standards

- Do not share Sligo Social Services passwords with anyone, including suppliers, external trainers or sponsors. All passwords are to be treated as sensitive and confidential information.
- Do not reveal a password in email, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password (e.g., "my family name").
- Do not reveal a password on questionnaire or security forms.
- If someone demands a password, refer them to this document and direct them to the I.T, Administrator.
- Always decline (select No) the use of the "Remember Password" feature of any applications (e.g.

websites, Eudora, Outlook, Netscape Messenger).

- Do not reuse old passwords

If an account or password compromise is suspected, report the incident to the I.T. Administrator who will immediately make changes.

C. Use of passwords and passphrases for Remote Access Users

Access to Sligo Social Services Network/PC's via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

D. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is therefore, more secure. A passphrase is typically composed of multiple words, because of this, a passphrase is more secure against "dictionary attacks".

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficON The 101 Was8&#This Morning"

All of the rules above that apply to passwords apply to passphrases.

E. Password Storage

Password Encryption

A single folder containing passwords for every webpage or application both at system and user levels is to be encrypted.

Any employee found to have violated this policy may be subject to disciplinary action by management. Password cracking or guessing may be performed on a periodic or random basis by the I.T. Administrator. If a password is guessed or cracked during these exercises, the user/owner will be required to change it.

Working Remotely

Sligo Social Services acknowledges that some employees may be required to work outside of the office from time to time. During this time there is a heightened risk of data breaches therefore employees must take very seriously their responsibly to ensure that this does not happen. Sligo Social Services expects employees to continue to use common sense, ensuring that great care is taken of people's names, addresses and more sensitive data. Sligo Social Services realises that working from home or outside of your regular office environment can place you in a different mental space from your usual workspace. Therefore, it is important that every employee of Sligo Social Services adheres to the following:

Devices

- Employees must continue to use common sense and make sure that you are taking care of things like people's names and addresses. Take particular care for more sensitive data, such as information about persons' health, political or trade union affiliation, or religion.
- Remember that working from home can place you in a different mental space from your usual work space.
- Employees working from home will not store sensitive data on laptops, home computers, removable storage devices or any IT device that is not stored in the office, encrypted and backed up to the cloud.
- Staff may, after agreeing temporary remote working arrangements with their manager/supervisor connect remotely to their office desktop.
- If using a laptop, you must ensure it is equipped with a strong password and is encrypted.
- Maintain privacy at all times. Your work files, emails and databases should not be used where visible to family members or housemates, or left open and unattended.
- Work computers such as laptops should never be used by family members or for non-work purposes.
- You must lock your device if you have to leave it unattended for any reason. Ensure your device is turned off, locked and stored carefully when not in use.
- Ensure that all devices including phones and laptops are not lost or misplaced. If this happens, you must report it immediately to your manager/supervisor to ensure a remote memory wipe where possible.

Emails

- Be familiar with and adhere to Sligo Social Services email policy.
- Use work email accounts rather than personal ones for work related emails involving personal data. Avoid using personal or confidential data in subject lines.
- Continue to double check address and attachments when using email and always use the BCC function for group emails.

Paper Records

- Employees will not take out of the secure environment of the office any file containing sensitive information.

- Employees will only remove confidential information from the secure environment in the following circumstances:
    - Where no alternative arrangement is possible
    - Where specific permission has been granted by the Line Manager

Sensitive Data Definition: Data consisting of racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.

Personal Data Definition: Personal data' means 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;

Video Conferencing

Sligo Social Services has video conferencing arrangements in place for some staff who need to join meetings but may be working out of office. Video conferencing allows employees of Sligo Social Services to meet together and share ideas and images while not necessarily in the same room. Video conferencing allow managers and supervisors to conduct face-to-face meetings with employees who may work remotely or in another part of the region.

The Data Protection Commissioner has recognised the need for specific guidelines regarding the use of video conferencing and have set out some tips on how we should seek to comply with GDPR when utilising these services.

- Ensure that the device you are using out of office is making the necessary updates, such as operating system updates (like iOS or android) and software/antivirus updates.
- Authorisation must be sought and agreed by manager/supervisor before use of the video conferencing app.
- Staff must, before undertaking any video conferencing on behalf of the organisation, ensure they are familiar with and understand all policies and guidelines relating to Data Protection and Video Conferencing, in order to minimise data protection risks.
- Think twice about what permissions for data or sensors you are being asked for: Do not share your location or your list of contacts.
- Be wary of services that may ask for access to your device. Do not give access to your device.

- Ensure your device is used in a safe location, for example keep an eye on what (or who) can be seen from your camera, and be sure to log out, mute, or turn off video, as appropriate, when you leave or take a break.
- Consider the data protection and privacy rights of others. Do not record meetings. Do not post or share a picture or video of a video-call that contains their image, voice, and/or contact details.
- Video conferencing will not be used for personal calls.
- Employees should not use outside services to fix IT problems but should contact the office for help. If the office cannot sort the problem, they will give you the phone number of a person you can call.
- You must always use work accounts, email addresses, phone numbers, etc. for work-related videoconferencing, to avoid the unnecessary collection of personal contact or social media details.
- During video conferencing avoid sharing of company data, document locations or hyperlinks in any shared 'chat' facility that may be public.

It is important to note that a video conference is no different from having a meeting in your own office with the door closed. Your meeting is confidential, whether you are hosting the meeting or simply joining a meeting. Therefore, you must ensure that you conduct all video conferencing meetings away from anyone else's gaze and out of earshot.

APPENDIX 1 DATA PROCESSING AGREEMENT

Dated:

Parties:

(1) Sligo Social Service Council CLG, a registered charity (number 20024390), main office at Charles Street, Sligo is the Data Controller.

And

(2) [Name of Data Processor] of [Address] is the Data Processor **Background**

(A) The Data Controller uses the services of the Data Processor from time to time to [insert activity e.g. IT Technician, Web hosting services etc.].

(B) The Parties have agreed to enter into this Agreement to ensure compliance with the General Data Protection Regulations (GDPR) in relation to all such processing.

(C) The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards.

1. Interpretation

The terms and expressions set out in this agreement shall have the following meanings:

"Act" means the General Data Protection Act (GDPR)

["Contract" the agreement between the parties for [insert subject matter of the agreement] dated [insert date];]

"Data Controller" is Sligo Social Service Council CLG

"Personal Data" shall include all data relating to individuals which is processed by the Data Processor on behalf of the Data Controller in accordance with this Agreement.

It is agreed as follows:

2. [This Agreement sets out various obligations in relation to the processing.]

   OR

   [The terms of this Agreement are to apply to all data processing carried out for the Data Controller by the Data Processor and to all personal data held by the Data Processor in relation to all such processing whether such personal data is held at the date of this Agreement or received afterwards. The terms of this Agreements shall supersede any previous arrangement, understanding or agreement between the parties relating to data protection.]

3. The Data Processor is to [carry out [describe services as in (A) above], and process personal data received from the Data Controller only on the express instructions of designated contacts at the Data Controller.

4. The Data Processor shall comply at all times with the Act and shall not perform its obligations under this Agreement in such a way as to cause the Data Controller to breach any of its applicable obligations under the Act.

5. As personal data provided to the Data Processor by the Data Controller or obtained by the Data Processor in the course of its work with the Data Controller is strictly confidential and will not be copied disclosed or processed in any way without the express authority of the Data Controller.

6. The Data processor agrees to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation.

7. Where the Data Processor processes personal data (whether stored in the form of physical or electronic records) on behalf of the Data Controller shall:

7.1 process the personal data only to the extent, and in such manner, as is necessary in order to comply with its obligations to the Data Controller;

7.2 Implement appropriate technical and organisational measures and take all steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply details of such measures as requested from the Data Controller;

7.3 [In furtherance of its obligations under 7.2 above implement and maintain the security measures set out in Schedule 1 of this agreement];

7.4 If so requested by the Data Controller (and within the timescales required by the Data Controller) supply details of the technical and organisational systems in place to safeguard the security of the personal data held and to prevent unauthorised access;

7.5 On reasonable prior notice, permit persons authorised by the Data Controller to enter into any premises on which personal data provided by the Data Controller to the Data Processor is processed and to inspect the Data Processor's systems to ensure that sufficient security measures are in place;

7.6 Notify the Data Controller (within two working days) if it received:

7.6.1 A request from a data subject to have access to that person's personal data; OR
7.6.2 A complaint or request relating to the Data Controller's obligations under the Act;

7.7 Provide the Data controller with full co-operation and assistance in relation to any complaint or request made, including by:

7.7.1 Providing the Data Controller with full details of the complaint or request;
7.7.2 Complying with a Data Access Request within the relevant timescale set out in the Act and in accordance with the Data Controller's instructions;
7.7.3 Providing the Data Controller with any personal data it holds in relation to a Data Subject (within the timescales required by the Data Controller);
7.7.4 Providing the Data Controller with any information requested by the Data Controller;

7.8 Not transfer any personal data provided to it by the Data Controller to any third party without the written consent of the Data Controller and ensure that any third party to which it sub-contracts any processing has entered into an Agreement with the Data Processor which contains all the obligations that are contained in this Agreement and which permits both the Data Processor and the Data Controller to enforce those obligations.

8. The Data Processor agrees that in the event that it is notified by the Data Controller that it is not required to provide any further services to the Data Controller under this Agreement. The Data Processor shall transfer a copy of all information (including personal data) held by it in relation to this Agreement to the Data Controller in a format chosen by the Data Controller and/or, at the Data controller's request, destroy all such information using a secure method which ensure that it cannot be accessed by any third party and shall issue the Data Controller with a written confirmation of secure disposal.

9. All copyright, database right and other intellectual property rights in any personal data processed under this Agreement (including but not limited to any updates, amendments or adaptations to the personal data by either the Data Controller or the Data Processor) shall belong to the Data Controller. The Data Processor is licensed to use such data only for the term of and in accordance with this Agreement.

10. [The Data Processor accepts the obligations in the Agreement in consideration of the Data Controller continuing to use its services.]

Signed for and on behalf of Sligo Social Service Council CLG by:

_____ _____

Print Name Signature

_____

Position

Signed for and on behalf of [Name of Data Processor] by:

_____ _____

Print Name Signature

_____

Position

Data Processing Agreement Schedule 1

1. The Data Processor will ensure that in respect of all personal data it received from or processes on behalf of the Data Controller it maintains security measures to a standard appropriate to:
   - the harm that might result from unlawful or unauthorised processing or accidental loss, damage or destruction of the personal data;
   - the nature of the personal data.

2. In particular the Data Processor shall:
   - have in place and comply with a Data Protection Policy and Data Protection Impact Assessment which:
     - defines security needs based on a risk assessment ○ allocates responsibility for implementing the policy to a specific individual or members of a team;

- is provided to the Data Controller on or before the commencement of this Agreement; ○ is disseminated to all relevant members, volunteers and staff; and provides a mechanism for feedback and review.

- Ensure that appropriate security safeguards and virus protection are in place to protect the hardware and software which is used in processing the personal data in accordance with best industry practice;

- Prevent unauthorised access to the personal data;

- Ensure its storage of personal data conforms with best practice such that the media on which personal data is recorded (including paper records and records stored electronically) are stored in secure locations and access by personnel to personal data is strictly monitored and controlled;

- Have secure methods in place for the transfer of personal data whether in physical form (for instance, by using couriers rather than post) or electronic form (for instance, by using encryption);

- Put password protection on computer systems on which personal data is stored and ensure that only authorised personnel are given details of the password;

- Take reasonable steps to ensure the reliability of any members, volunteers and employees or other individuals who have access to the personal data;

- Ensure that any employees or other individuals required to access the personal data are informed of the confidential nature of the personal data and comply with the obligations set out in the Agreement;

- Ensure that none of the employees or other individuals who have access to the personal data publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the Data Controller;

- Have in place methods for detecting and dealing with breaches of security (including loss, damage or destruction of personal data) including:

    - The ability to identify which individuals have worked with specific personal data; ○ Having a proper procedure in place for investigating and remedying breaches of the data protection principles contained in the Act; and ○ Notifying the Data Controller as soon as any such security breach occurs.

- Have a secure procedure for backing up and storing back-ups separately from originals;

- Have a secure method of disposal of unwanted personal data including for back-ups, disks, printouts and redundant equipment.

APPENDIX 2 Data Sharing and Usage Agreement

This agreement establishes the terms and conditions under which Sligo Social Service Council CLG and any recipient can acquire and use data for an agreed purpose from the other party. Either party may be a provider of data to the other, or a recipient of data from the other.

1. The confidentiality of data pertaining to individuals will be protected as follows:
    a. The data recipient will not release the names of individuals, or information that could be linked to an individual, nor will the recipient present data in any manner that would reveal the identity of the individuals.
    b. The data recipient will not release individual addresses, nor will the recipient present data in any manner that would reveal the addresses.
    c. Both parties shall comply with the relevant Irish legislation, namely the Irish Data Protection Act (1988), the Irish Data Protection (Amendment) Act (2003), and the General Data Protection Regulation (GDPR) (2018).
2. The data recipient will not release data to a third party without prior approval from the data provider.
3. The data recipient will not share, publish, or otherwise release any findings or conclusions derived from analyses of data obtained from the data provider without prior approval from the data provider
4. All data transferred to the recipient will remain the property of the data provider.
5. Any third party granted access to data, as permitted under condition 2 above, shall be subject to the terms and conditions of this agreement. Acceptance of these terms must be provided in writing by the third party before data will be released.

Sligo Social Service Council CLG and the Recipient have hereunto executed this Data Sharing Agreement as of the date written below.

_____

Signed on behalf of Sligo Social Service Council CLG

Date:_____

_____

Signed by Recipient

Date:_____

APPENDIX 3 Privacy Statement

Sligo Social Services is committed to complying with the terms of the General Data Protection Regulation 2018, and to the responsible and secure use of your personal data. Sligo Social Services has a legitimate interest in processing personal data in order to provide adequate and appropriate services.

Information about you

Sligo Social Services collects personal information from you when you start receiving a service. A file is set up which includes your contact details and other relevant personal information. Once you finish receiving a service, the file is closed, safely stored and after being held for an appropriate length of time, the file will be destroyed under confidential conditions.

Our use of this information

Your personal information will be used only to provide you with appropriate services. We will not share your personal details with any other person or organisation without your knowledge and permission, unless there is a legal requirement, if there is a child or adult safeguarding issue, or a perceived risk of harm. A breach of confidentiality is when a person shares information with another in circumstances where it is reasonable to expect that the information will be kept confidential.

Security

We will take all reasonable precautions to prevent the loss, misuse or alteration of information you give us.

Your rights over your personal data

If you would like to see the information we hold about you, or would like to correct, update of delete any records, or if you have any concerns about our use of your data, please email us at info@sligosocialservices.ie.

APPENDIX 4

Service User Information and Consent Form

In order for Sligo Social Services to provide you with adequate and appropriate services it is necessary for us to collect information from you which will be recorded on your file. Information will be stored electronically and manually. All information will be held in accordance with the seven principles contained in Article 5 of the General Data Protection Legislation (GDPR) 2018.

Personal data shall be:

a) **Lawful, fair and transparent processing** – Sligo Social Services processes personal data based on lawful processing conditions. You are entitled to have full and transparent knowledge of the identity of the parties to the processing, the purposes of the processing, the recipients of personal data, the existence of your rights and freedoms, and how to contact the Controller.

b) **Specified and lawful purpose** – your personal data will be processed only for a specified purpose.

c) **Minimisation of processing** – processing of your personal data will be adequate, relevant and restricted to what is necessary in relation to the purposes for which it is processed.

d) **Accuracy** – your personal data shall be accurate and where necessary kept up to date. Sligo Social Services will rectify any incorrect data and erase any data, which is known to be erroneous or obsolete.

e) **Storage limitations** – your personal data shall be kept in a form which permits your identification for no longer than is necessary for the purposes for which your personal data is processed.

f) **Security and confidentiality** – Sligo Social Services will employ high standards of security in order to protect the personal data under its care. Sligo Social Services Password Policy, Data Sharing and Confidentiality Agreement and Data Retention and Destruction Policy guarantee protection against unauthorised access to, or alteration, destruction or disclosure of any personal data held by Sligo Social Services in its capacity as Data Controller. Access to and management of staff and client records is limited to those staff members who have appropriate authorisation and password access. Sligo Social Services will carry out regular internal security audits.

g) **Liability and accountability** – The Data Controller and the Data Processor will comply with the General Data Protection Regulations (GDPR). The Data Controller will exercise reasonable care to ensure that the Data Processor carries out the processing in strict compliance with the GDPR.

Who sees the Information?

Sligo Social Services staff have a duty of confidentiality and there are strict rules about who will have access to your record. All computers are encrypted and password protected and all files are stored in secure locations and access by personnel to personal data is strictly monitored and controlled.

Is my consent required? You must give consent to allow Sligo Social Services to process your personal data. You will give consent by signing at the end of this form. You have the right to reverse the decision of consent if you so wish.

What if I refuse to give consent?

It is your right to refuse to give consent, and this will not exclude you from receiving a service.

Can I see or have a copy of information recorded about me?

You have the right to access personal data that was collected about you, and only you. You must make a request in writing and Sligo Social Services will respond to your request within 30 days. You have the right to know what data is being held relating to you, where the personal data is being processed, purpose of processing and how long this data will be stored.

Is my information kept confidential?

Your personal information will be processed in a manner that ensures appropriate security of personal data, including protection against unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Can I have information about me changed?

Personal data held by Sligo Social Services will be accurate and where necessary kept up to date. Sligo Social Services will rectify any incorrect data and erase any data, which is known to be erroneous or obsolete.

Will you send automated emails?

Sligo Social Services will not send emails to promote commercial products. However, you may receive transactional emails which are not promotional in nature, and might be used as a communication tool for an agreed purpose such as receipts, or reminders.

Will you telephone or text me?

Sligo Social Services will not telephone or text you unless for an agreed purpose?

Note: You have the right to make a complaint to the Data Protection Commissioner if you are unhappy with how Sligo Social Services is discharging its duties under the Data Protection Act.

Consent Form

I consent to have information recorded about me and my use of services.

I understand that this information may be shared with other services as necessary.

I consent to receive transactional emails, telephone calls and texts for an agreed purpose.

I have been informed of my rights to access all information recorded about me.

Signed: _____

Dated: _____

Witnessed by: _____

Service: _____

Position: _____

Date: _____

APPENDIX 5 Subject Access Request Form

Sligo Social Service Council CLG

*Date issued to data subject*_____

Access Request Form: Request for a copy of Personal Data under Irish legislation, namely the Irish Data Protection Act (1988), the Irish Data Protection (Amendment) Act (2003), and the General Data Protection Regulation (GDPR) (2018).

Important: Proof of identity must accompany this Access Request Form (e.g. official photographic identity document such as driver's licence, passport).

Full Name	
Maiden Name (if changed since accessing service)	
Address	
Contact Number	Email Address

**We may need to contact you to discuss your access request*

I,_____[insert name] wish to be informed whether or not Sligo Social Service Council CLG holds personal data about me or my child and to be provided with a description of this data and to be informed of the purpose for holding such data. I am making this access request under Article 5 of the General Data Protection Regulation (GDPR) 2018.

☐

OR

I,_____[insert name] wish to make an access request for a copy of any personal data that Sligo Social Service Council holds about me or my child. I am making this access request under Article 15 of the General Data Protection Regulation (GDPR) 2018.

☐

Signed:_____ Dated:_____

Please return this form to The Data Controller, Sligo Social Service Council CLG, Charles Street, Sligo.

APPENDIX 6 Personal Data Breach Report Form

If you discover a data security breach, please notify the manager immediately. Please complete form below and return to the relevant manager.

Date(s) of breach:	
Date Incident was discovered:	
Name of person reporting incident:	
Brief description of Personal Data Security Breach:	
Number of Data Subjects affected – if known:	
Brief Description of any action since breach was discovered:	
Was Incident reported to the Data Subject? If not, why not?	
Was incident reported to the Office of the Data Protection Commissioner? If not, why not?	
Breach Identified By: signature	
Office Use Only	
Report received by: signature	
Date:	
Action:	
Date	

APPENDIX 7

Data Retention Periods

Financial Records	Retention period	Final action
Financial Records		
• Invoices • Tax Records • Tax Clearance Certs • Debtors Ledger • Income Listings • Receipts Reconciliations • Bank Reconciliations • Bank Statements • Credit Card Records • Fixed Assets Register • Depreciation Schedules • Audit Reports • Cancelled Cheques • Travel Claims • Receipt Books • Purchase Orders • Food Voucher Book Stubs • Petty Cash Books	Current year plus 10 Years	Confidential Shredding Remove from Server
Property Records		
• Deeds and titles of properties/assets • Maps • Plans • Drawings • Records of sales and purchases of Sligo Social Services properties	Perpetuity	Archive in original form
• Lease Agreements	Current year plus 7 Years	Confidential Shredding
Insurance Records		
• Insurance Claim Documents	Current year plus 5 Years	Confidential Shredding
• Accident/injury Report	Current year plus 2 Years	Confidential Shredding
Other Records		
Invitation to Tender documents	Hold for 3 years after award of contract	Confidential Shredding
Payroll		

• Pension records	Until individual is 70 years or if dispute hold until resolved	Confidential Shredding Remove from Server
• • Authorisation to deduct from Pay • Payslips Payroll records	Current year plus 10 Years	Confidential Shredding

Personnel Records	Retention Period	Final Action
Personnel – Recruitment		
• Applications for vacant post • Candidates not short listed • Candidates short listed but not successful • Advertisements • Job Description • Interview Records • Correspondence • Offer	2 years unless candidate successful then hold for current year plus 7 years after resignation or retirement	Confidential Shredding Remove from server
Personnel – Staff File		
• Application form/curriculum vitae • Letter of application • Interview notes • Letter of offer • Contract of employment • Employment references • Next of kin details • Change of address forms • Medical certificates in respect of sick leave • Police Vetting • Promotions, transfers, training, grievances and disciplinary matters, including investigations and warnings • Records relating to accidents at work • Correspondence	Current year plus 7 years after resignation or retirement	Confidential Shredding Remove from server
• Personnel spreadsheet • Attendance records	Current year plus 3 Years	Confidential Shredding Remove from server

Allegations and complaints Investigation unwarranted	Current year plus 2 Years	Confidential Shredding Remove from server
Employment Appeals Tribunal, Rights Commissioner, Labour Court, Equality Tribunal	7 years from completion of the case	Confidential Shredding
Supervision Notes	Held by Supervisor for duration of employment then scanned to CEO 's HR file to be held for Current year plus 7 years. If Supervisor leaves while staff member is still employed, then notes are transferred to CEO	Confidential Shredding Remove from server
Volunteer Files		
• Application Forms • References • Volunteer Contract • Job Specification • Training Record • Garda Vetting Disclosure • Proof of identity • Signed inviter form	Current year plus 7 years after cease volunteering	Confidential Shredding

Child Records	**Retention Periods**	**Final Action**
Client Files - Children		
Record of all visitors to schools	Current year plus 1 Year	Confidential Shredding
Attendance Register	Until youngest child listed in attendance register reaches 21 years	Confidential Shredding
Any accident, injury or incident record involving a child in the childcare service	Until child 21 years old for insurance. Once a child turns 18 they have a period of 3 years to make a claim over an incident that occurred in an early years if their parents have not already done so	Confidential Shredding
• Staff Rosters • Cleaning and HACCP records • Medication administered	Current year plus 2 Years	Confidential Shredding

Complaints received	2 Years after the complaint has been dealt with	Confidential Shredding
Fire record	Current year plus 5 Years	Confidential Shredding
Records of Yearly review of Service	Current year plus 3 Years	Confidential Shredding
• Child Observations • Child Development Records	Send home with family when child finishes unless you have a specific reason for keeping	Not applicable
Case File where the file contains: • Child Protection Issues • Welfare concerns • Children in foster care • Children placed for adoption	Perpetuity	Not applicable
No Child Protection Issues	Current year plus 7 Years from last contact with service	Confidential Shredding Remove from server
Database	Current year plus 2 Years after case is closed	Remove from server
Adult Records	**Retention Periods**	**Final Action**
Client Files – Adults		
Case files where file contains: • Child Protection Issues • Welfare concerns • Children in foster care • Children placed for adoption • Action under the 'Safeguarding Vulnerable Adults Policy' • Elder abuse • Retrospective disclosures of child abuse	Perpetuity	Not applicable
• No Child Protection Issues or issues in relation to Vulnerable adults	Current year plus 7 years from last contact with service	Confidential Shredding Remove from server

Organisational Records	Retention Periods	Final Action
Minutes of Board of Directors Meetings	Perpetuity	Archive
Personal details of Board members	Current year plus 7 years after ceased volunteering on Board	Confidential Shredding Remove from server
AGM Minutes	Perpetuity	Archive
Policies and Procedures signed off by Board of Directors	Until updated	Confidential Shredding Remove from server
• Supervisors Forum Minutes – master copy • Departmental Meetings – master copy	Current year plus 2 Years	Confidential Shredding Remove from server

General Admin	Retention Periods	Final Action
Quotes – Procurement	Current year plus 2 years	Confidential Shredding
Tradespersons Safety Statement and Insurance	1 year or until superseded by up-to-date copies	Confidential Shredding
Furniture Book	2 months	Confidential Shredding
Fire Systems Log	Current year plus 5 years	Confidential Shredding
Pest control log	Current year plus 2 years	Confidential Shredding
Diaries	2 Years	Confidential Shredding
CCTV Recordings	Retained for a maximum of 30 days	Automatically written over after 30 days
CCTV Log	2 Years	Confidential Shredding
Property Records	**Retention Periods**	**Final Action**
Title Deeds Maps Plans Drawings	Hold in perpetuity or until sale of property	Archive or hand over to new owners on sale of property

Appendix 8 File Storage and Destruction Register

Date	Data Subjects Name	Data Subject DOB	File ID Number	Hold in Perpetuity		Year for Destruction	Method of Destruction	Managers Signature
				Yes ✓	No ✓			

Appendix 9

Employee File Destruction Register

Employee Name	Date of Birth	Start Date	Finish Date	Department	Role	Date File Destroyed	Managers Signature
