KARE
Founded in 1967
Promoting Inclusion for People with Intellectual Disabilities

Data Protection / Records Management Policy.

KARE Policy Document.

Policy Owner: Data Protection Officer.

Rev. No.	Approved by the OMT	Approved by KARE Board	Launched at Heads of Units	Operational Period
This Policy replaces: Data Protection Policy July 2013 – Records Management Policy June 2014 – October 2017				
Rev.1	October 2017	October 2017	November 2017	November 2017 – April 2019
Rev 1.1	Jan 2019	March 2019	May 2019	May 2019 -
Rev 1.2	Approved by CEO 31st March 2021	N/A	By email 1st April 2021	April 2021 -
Rev 2	Nov 2021	N/A	Dec 2021	Dec 2021 -
Rev. No.	**Approved by the Policy Management Committee**	**Approved by KARE Board/Sub-Committee**	**Launched at Heads of Units**	**Operational Period**
Rev. 2.1	June 2022	N/A	June 2022	June
Rev 2.2	August 2022	N/A	Sept 2022	Sept 2022

Section 1: Policy

1.1 Background to this Policy

This policy has been developed to replace what were two separate policies on Record Management and Data Protection. The policy has been developed in line with best practice, and relevant legislation and regulation including:

- Freedom of Information Acts 1997, 2003 and 2018
- Data Protection Act 2018
- General Data Protection Regulation
- Data Sharing and Governance Act 2019

All KARE policies which include the management of information are relevant to this policy. Policies of particular relevance are:

- Use of Information & Communications Technology
- Use of CCTV and Monitors
- Staff Handbook
- Individualised Planning Policy
- Remote working policy

1.2 Aim of this Policy

The aim of this policy is to ensure that KARE keep accurate records of all its activities and decisions and that they are created, managed, shared, stored, and disposed of in accordance with General Data Protection Regulation (GDPR).

KAREs aim is to uphold and maintain the rights of each person's information treated in line with GDPR principles.

1.3 Definitions available in Appendix 3.

1.4 Scope of this Policy

KARE promote data protection as everyone's responsibility.

This policy applies to all KARE staff, CE and LTI participants, volunteers, students on placement and those working on behalf of KARE, including the Board of Directors.

This is an overarching policy in relation to all information created, received and maintained in order to carry out the business of KARE. It applies to records of all formats including,

- Paper based records
- Audio-visual records
- Electronic records i.e., records which are generated electronically and stored by means of technology.

Note: Data Protection Legislation states that consent cannot be sought from a child under the 'age of consent' which is 16 years; in such cases KARE will obtain consent from a person holding "Parental responsibility" for the child.

1.5 Policy Statements for Records Management of all types of Information

1.5.1 General Statements

1.5.1.1 KARE will ensure that records are kept in a manner which enables:

- Easy appropriate access to specific information in a timely manner
- KARE to perform its functions successfully, efficiently and in a legal and accountable manner
- Continuity of service in the event of a disaster

- Protection of the rights of all stakeholders including employees, people who use the service, volunteers, Board members etc.

1.5.1.2 Staff will ensure that all records are managed in accordance with this policy.

1.5.1.3 Staff will treat all records as important property of the individual and/or the organisation.

1.5.1.4 Records will be kept as long as is required for KARE business and in line with current legislation and regulation.

1.5.1.5 3rd parties contracted to provide a service to KARE will have a Data Processor/Joint Controller Agreement which clearly states how any records they have access to as part of the contract will be managed and who has ultimate ownership of them.

1.5.1.6 A Data Sharing Agreement will be established between KARE and public bodies/other service providers with whom is shares personal information for the purposes of carrying out its business. The Agreement will outline what data is being shared and how it will be used.

1.5.1.7 Line Managers will ensure that staff who report to them are trained in the creation and management of records as appropriate to their role. This is available on LEAP platform specific to KARE.

1.5.1.8 All Record Management systems will be developed and maintained in line with current best practice.

1.5.1.9 The system owner will ensure that record management systems are in place as appropriate to support the proper management of associated information in line with the organisational record management system.

1.5.2 Creation and capture of Records

1.5.2.1 Staff will create full and accurate records in accordance with agreed processes and procedures and in line with best practice.

1.5.2.2 Staff will ensure they use agreed formats for recording particular types of information including templates and reporting forms as relevant.

1.5.2.3 Staff should never alter a record so that the original record is no longer visible e.g., by erasing, deleting, removing, nor should they add content to the record later. Where a correction is required to a record, this should be done in a transparent way and the correction should be dated and signed.

1.5.2.4 Information should be developed professionally with the expectation that it will be accessed by a third party in the future.

1.5.3 Maintenance and Storage of Records

1.5.3.1 Staff will maintain and store records in accordance with agreed processes and procedures.

1.5.3.2 Staff will ensure that they move records from any temporary storage arrangement such as temporary files etc. into the relevant record management system at the earliest possible opportunity. (e.g., removed from desktop into KARE connect)

1.5.3.3 Non-electronic records will be kept in suitable storage conditions that ensure they are protected from damage.

1.5.3.4 Line Managers will ensure electronic records are stored appropriately KARE's systems.

1.5.4 Security of, and access to, Records

1.5.4.1 KARE will ensure that there are appropriate security/permission levels in place for all records and access to these records is based on a need for such information.

1.5.4.2 Staff will not disclose information or provide access to records to anyone who is not authorised to have such access.

1.5.4.3 Freedom of Information and Data access requests will be dealt with in accordance with the relevant legislation.

1.5.5 Retention and Disposal of Records

1.5.5.1 KARE will ensure that there are clear retention periods and methods of disposal for all record types in line with relevant regulation and legislation. A document of retention schedules will be managed by the Archive Administrator and held on KARE connect.

1.5.5.2 Line Managers will ensure all records in their area are retained and disposed of in line with this policy.

1.6 Policy Statements for Data Protection for Personal Information (GDPR General Date Protection Regulation).

1.6.1 Fair, lawful, and transparent processing of personal information (GDPR Principle 1) and Purpose limitation (GDPR Principle 2)

1.6.1.1 KARE process (e.g., capture, maintain, use, delete etc.) personal information about people to carry out its work. KARE will provide accessible information using the persons preferred method of communication to help people understand why we are doing this and how the information will be used.

1.6.1.2 If KARE needs to process an individual's personal information for any reason other than to carry out its work, KARE will get the permission of that individual or in the case of a child their representative. When the individual does not want this, their wishes will be recorded and respected.

1.6.1.3 When a person requires support to give or refuse their consent, they will be supported to make this decision in line with the total communication policy and the Assisted Decision-Making (Capacity) Act 2015.

1.6.1.4 KARE will only keep personal information for as long as necessary.

1.6.1.5 Where KARE keeps personal information on an individual, the individual has a right to:

I. know from where KARE got the information about them
II. know why KARE keeps information about them
III. know to whom KARE gives information about them
IV. know how KARE uses information about them to make decisions V. a copy of the information KARE keeps about them

A person can ask to see the information KARE keeps about them by contacting the relevant manager.

1.6.1.6 In a few cases, it may not be possible to give a person the information they ask for because KARE must follow the rules laid out in the current Data Protection legislation. (See

www.dataprotection.ie). The reason for not sharing information will be made clear to the requester.

1.6.1.7 KARE will ensure that any personal information will only be processed for specified, explicit and legitimate purposes.

1.6.2 Ensuring personal information is adequate, relevant and not excessive (GDPR Principle 3)

1.6.2.1 As part of the standard Process Review, Process Owners in KARE will review the personal information gathered by that Process and make sure it is only what is needed for that process through the data processing log (needs to include the process owner).

1.6.2.2 Any new data handling processing systems needs to have a DPIA conducted by the process owner and signed off by the DPO.

1.6.2.3 All people executing DPIAs need to have completed the HSELanD module on the 'Fundamentals of GDPR'.

1.6.2.4 If a staff member thinks something should be changed about how personal information is processed, they should inform their Line Manager, who will in turn talk to the department manager/ Process Owner and ask them to review this practice.

1.6.3 Keeping personal information accurate, complete, and up to date (GDPR Principle 4)

1.6.3.1 Line Managers will make sure personal information held in their area is kept accurate and up to date.

1.6.3.2 Staff members will ensure they maintain accurate records which are kept up to date.

1.6.3.3 KARE will ensure that periodic reviews/audits are carried out to ensure that personal information held is accurate and up to date.

1.6.3.4 Any individual has a right to have any inaccurate information about them corrected or erased. To do this the individual should contact the relevant manager, asking for the

inaccurate information to be corrected or deleted. They should give reasons and be able to prove that the information is wrong. The line manager will follow up on the request to ensure records of the request and rational for accepting/refusing the request are maintained accurately. The line manager can seek clarification from the DPO if required. Records of these exceptional requests will be maintained by the DPO.

1.6.4 Retention and Disposal of personal information (GDPR Principle 5)

1.6.4.1 KARE will maintain Record Retention schedules which set out how long personal information should be kept and how KARE will dispose of it. Attached schedule link available in Appendix 2.

1.6.4.2 Records will be destroyed in a way that is irreversible and ensures there is no reasonable risk that the information may be retrieved, e.g., shred paper records, delete computer-based records from the recycle bin, certified destruction of computer hard drives from old equipment.

1.6.4.3 When current shredding machines need to be replaced, the new machines purchased must be of a high spec in line with P3 standard for shredding machines.

1.6.5 Keeping personal information confidential, safe, and secure (GDPR Principle 6)

1.6.5.1 KARE will keep personal information safe and secure by:

- Securely locking non-electronic personal information away when not in use.
- Storing electronic information on KARE's servers, secure cloud systems, password protected PCs or encrypted laptops.

- Not putting any personal information on memory sticks, even temporarily.
- Using passwords/PINs on computers and smart phones
- Immediately downloading any photos or videos onto password protected computers and deleting them from phones or camera/camcorder
- Following KARE's guidelines when using email, fax or when talking about people on the phone or in person
- Not having personal information stored in public areas.

1.6.5.2 Staff will have restricted access to information based on their role. Students on placement in KARE may be given have access to personal information, the level of access will be based on their placement objectives and will be approved by the Line Manager. The person will be made aware of the sharing of this information.

1.6.5.3 Companies contracted by KARE to process personal information will have a Data Processing Agreement in their contract governing the processing of personal information and detailing their responsibilities.

1.6.5.4 When staff share personal information with relevant people in KARE, they will only tell them the information they need to know, at the time they need to know it and nothing more.

1.6.5.5 Staff will only share an individual's personal information with someone outside of KARE with permission from that individual. However, staff may need to share personal information without permission from the individual in certain circumstances such as:

- If they are in immediate danger
- medical emergency
- law or court order
- concern of abuse or neglect

1.6.5.6 A staff member will talk to their Line Manager if they are unsure about using or sharing personal information. Staff will follow technical security measures around any information they transfer as outlined in the procedures below.

1.6.6 Ensuring Accountability for Data Protection (GDPR Principle 7)

1.6.6.1 KARE will have a named person to act as Data Protection Officer, see Appendix 1

1.6.6.2 KARE will keep relevant logs and assessments in line with the requirements of GDPR such as Processing Logs and Data Protection Impact Assessments.

1.6.6.3 KARE will provide training for staff to help them understand how best to manage and protect personal information.

1.6.6.4 Staff will inform their Line Manager as soon as possible after they become aware that personal information has been lost, stolen or shared with somebody not entitled to it. They will also report the incident on the Data Breach Report

1.6.6.5 The Data Protection Officer will review Data Breaches in consultation with relevant others and decide on the actions required in line with GDPR requirements.

1.6.6.6 Line Managers will ensure an individual and/or their representatives whose personal information has been lost, stolen or shared with somebody not entitled to it, is informed of the breach, in line with the principles of Open Disclosure.

Section 2: Procedures and Guidelines

2.1 Guidelines on the Creation and Capture of Records

- Records may be created in any format, including paper, electronic or digital media, as long as their usability, reliability and integrity can be preserved for as long as the record is needed.
- Electronic records under preparation will be marked as draft and where relevant a version number until such time as they are finalised, at which point draft will be removed and they will have become a finalised record.
- Records must be accurate and complete, so that it is possible to establish what decisions and actions have been taken, and why.
- Records should be created at the time of, or as soon as practicable after, the event or transaction to which they relate to ensure they are accurate and reliable. Adverse events should be documented by the staff member who witnessed the incident or by the first staff member who was notified about it. Any amendments to an incident report should be discussed with the line manager in advance of any change. It may be appropriate to add a document to the adverse event or document a contact note as opposed to altering the original record. Should an amendment to an adverse event be required, the formal amend request feature should be used within KARE.
- Duplicate records or multiple copies of the same record should be kept to a minimum. There is normally only a need to retain one 'master' copy of each record.
- 'Convenience copies' may be required by individuals for a short period of time i.e., copy of papers/agenda when attending a meeting. However, these should be destroyed as soon as they are no longer required.
- Should a correction need to be made, brackets will be placed around the words to be corrected and a line drawn through them so that the original entry is still visible. The error should be signed and dated.
- All records should be named and dated so that their contents can be easily identified without opening the document/ file.
- Only use own log in details in line with ICT policy.

2.2 Keeping Personal, Sensitive or Confidential Information safe and secure

- Put any paper files or records that contain personal, sensitive, or confidential information into a locked drawer/cupboard/filing cabinet when you are finished using them .

- Take care to ensure that others calling to your desk/area where you are working cannot see personal, sensitive, or confidential information.
- Keep all drawers/cupboards/filing cabinets that contain personal, sensitive, or confidential information locked when unattended.
- Make sure to secure files/records that contain personal, sensitive, or confidential information when leaving your desk for extended periods and at the end of each day by putting them into a locked drawer/cupboard/filing cabinet or by locking the office. • Keep keys for rooms and drawers/cupboards/filing cabinets in a secure place.
- Shut down or lock your PC/laptop (you can lock it by pressing Ctrl+Alt+Del and choosing ‘Lock’) when you are leaving it unattended.
- Do not share your PC/laptop encryption code or password or system passwords with anyone.
- Transfer and delete personal, sensitive, or confidential information from portable devices such as smart phones, cameras etc. as soon as possible.
- Sensitive and confidential information should either be delivered in person or stored electronically where it can be accessed by those who need it whenever possible rather than sending it through the internal post or by email.
- Electronic information should be stored securely in an organised file structure.
- Be careful not to discuss personal or sensitive information about an individual in a place where the discussion can be overheard by others.
- Only discuss personal, sensitive, or confidential information on the phone when necessary. Always confirm who you are speaking with before disclosing information.

- Where possible do not use a person's full name or any other identifying information when referring to them on a phone call.
- Do not use text messages to communicate personal, sensitive, or confidential information.
- Only leave a voicemail message when absolutely necessary. If you need to leave a voicemail, leave the minimum amount of information. Things to consider: Who are you talking to? What information do they want/need? Why do they need it? What impact might disclosing this information have?
- Mail containing sensitive personal information should be clearly marked as confidential.
- Use registered post when sending particularly sensitive information by post, this will facilitate tracking and proof of delivery.
- Any information travelling in hard copy in relation to a person we support, staff member or volunteer will be protected in line with this policy.
- Staff remote working need to apply these same principles to data management.
- Sharing of confidential information should only be done in consultation with line manager and process owner as appropriate.

2.3 Using Email/Fax to communicate sensitive or personal information

- Any information of a personal nature being sent externally should be encrypted as outlined in 2.3.1 below.
- Any new process where information is being routinely being exchanged between KARE and other parties requires a DPIA to be completed and may require an additional agreement to be completed based on the outcome of DPIA. See 2.8.3 below for further details.
- Systems designed to hold personal information should be used for that purpose in the first instance and kept from being repeated in email correspondence e.g. email may refer staff to review Adverse event on CID but not contain any details.
- Before using email to communicate personal information consider an alternative more secure way of sharing the information e.g. using the share facility on Team site, OneDrive, MS teams or using KARE CID.

- When it is necessary to send any personal information by email all references to services users should be made by using their KARE ID where this is possible. Otherwise use initials or first name and initial of surname.
- When it is necessary to send sensitive, personal or confidential information by email take care to file the email and any attachments in an appropriate way i.e. in a folder system in Office 365 or by 'printing' to PDF and saving in the appropriate electronic system.
- When personal, sensitive or confidential information is sent via email and subsequently filed appropriately the email needs to be deleted from the senders email account.
- When personal sensitive or confidential information is received via email and subsequently filed appropriately the email needs to be deleted from the receiver's email account.
- Do not put personal, sensitive or confidential information in the body of an email.
- Do not send an email which contains personal, sensitive or confidential information to a general email address that multiple people can access e.g. a Local Service address. Send it to a named staff members email address.
- Do not send an email which contains personal, sensitive or confidential information to anyone, without the confirmed consent of the individuals or their representatives through the service agreements. There may be additional requests outside the service agreement which will be done on a case-by-case basis.
- Ensure all information is only sent to the parties who need to receive the information.
- Use Bcc (blind copy) if sending an email to multiple people using their personal email addresses.
- Always double check that the email is addressed to the correct person before sending. Use the prompts to check before sending outlined below in appendix 4.
- Be especially careful if using the Reply button that it is only going to the people you want to communicate with. Use the prompts to check before sending outlined below in appendix 4.

- If you receive an email and you are not the intended recipient, contact the sender as soon as possible to notify them of the error, then delete/ destroy the information.
- A Fax with sensitive information should not be left unattended in the machine, ensure that a person is waiting to receive it on the other end.
- Keep a copy of the Fax transmission report in the person's file.

2.4 Sending personal and sensitive information externally via email

Details available in (Appendix 4)

2.4 Printing personal, sensitive, or confidential information Details available in Appendix 7.

2.6 Transporting Files/Records containing personal, sensitive or confidential information

- Only take files containing personal, sensitive or confidential information out of their usual location when absolutely necessary and if you are authorised to do so.
- Carry/transport records in a way that ensures the individual's name/s are not visible.
- When transporting records containing personal, sensitive or confidential information do what is practicable to keep them safe and secure at all times.
- Never leave records containing personal, sensitive or confidential information unattended.
- Records being transported for delivery to another KARE department/location should be delivered to the appropriate person as soon as possible.
- As a general rule, do not transport files or records if possible and look to see if an alternative solution is available.

2.7 Reporting and managing an incident where personal information has been lost, stolen, or shared with somebody not entitled to it.

- The following can be classed as a breech and must be reported upon in line with drop down menu on CID for a data breach:
- Misplaced information that has not been recovered.
- Misplaced IT equipment.
- Disclosure of information, communicating in any format, personal information to unauthorised people. Emails sent to the wrong person/s containing any personal, sensitive, or confidential information. Photographs, sending personal info which has not been encrypted.
- Transmission / storage of information. For example, corruption of information during electronic upload/ download, information is stored on an application that fails to follow basic security practices.
- Destruction of information.
- Altered information. For example, a hacker breaks into an organization's HR database and replaces their employees' bank account numbers with his own. This counts as one form of **data alteration**.
- Access to stored personal information. For example, download or viewing **of data** by someone who isn't authorized to **access** it.
- Unauthorised shared. For Example, an **unauthorised** person gaining access to your laptop, email account or computer network. sending an email with personal data to the wrong person.
- Unavailability of information. For example, the sort of problem that might arise after a cyberattack that prevented access to and/or destroyed records

2.7.1 Tell the Line Manager as soon as possible

2.7.2 Work with the Line Manager to establish the detail of the breach including:

- the date and time of the incident and when it was discovered
- who discovered/reported the incident?
- exactly what happened
- Who and what was involved e.g., other people, ICT systems etc.?
- any particular evidence

2.7.3 Report the incident to the Data Protection Officer as soon as possible and complete a Data Breach Notification Form on CID. Provide as much information as possible in the report in line with 2.5.2 and including what were the first steps undertaken.

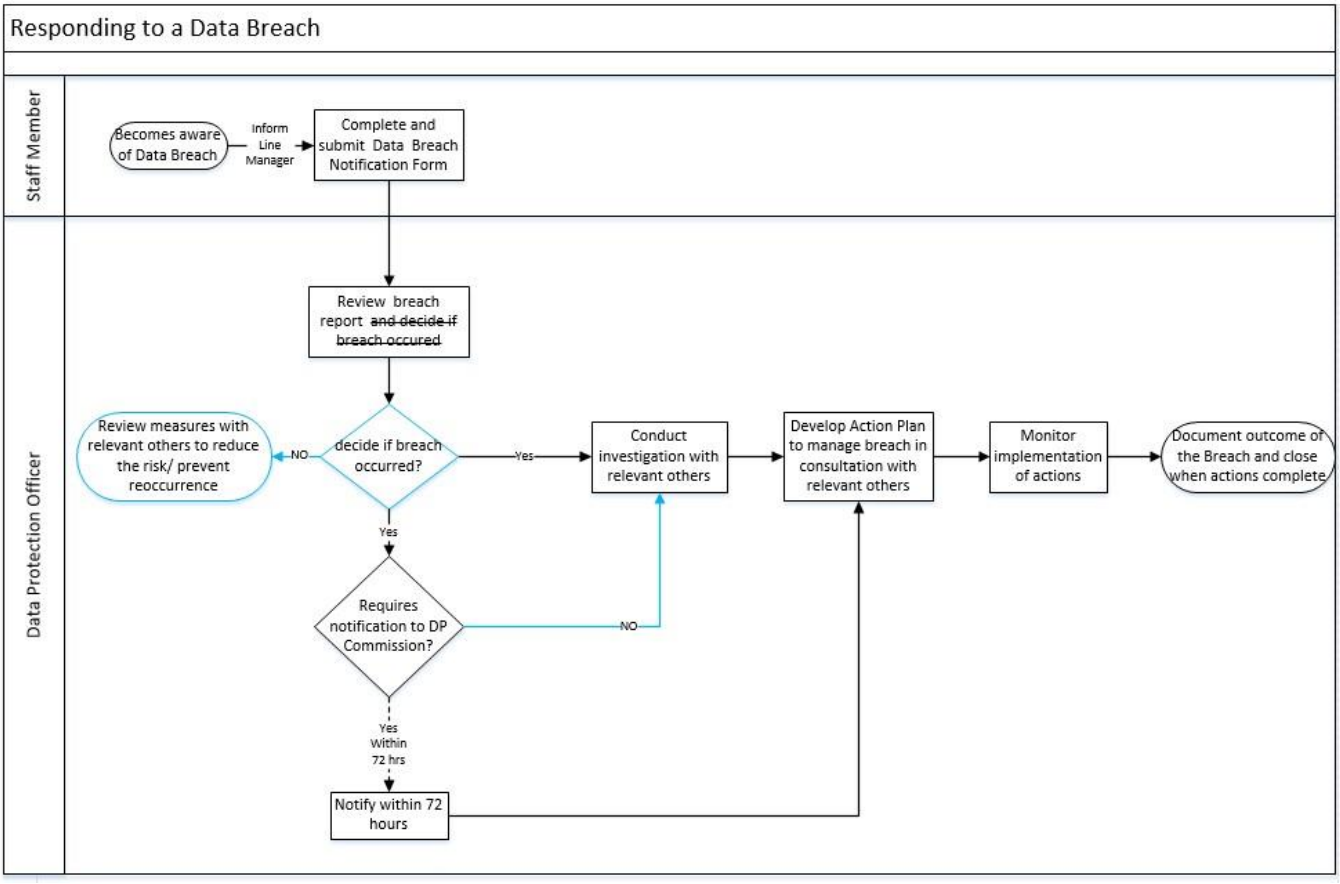
2.7.4 The Data Protection Officer and relevant others will work together to investigate the breach and decide what action needs to be taken including:

- who else in the organisation needs to be told about the incident?
- what should be done to recover the information or limit the damage caused
- how to tell the individual(s) who need to be informed that their information that has been lost, stolen or given to somebody not entitled to it.
- What external bodies need to be told about the breach such as the Data Protection Commissioner
- They will use the guidelines set out on the Data Protection website (www.dataprotection.ie) to help them make the right decisions.
- The DPO will complete the necessary responses to the follow up questions on KARE CID and identify who was involved in making the decision.

2.7.5 Where relevant the Data Protection Officer will inform the Data Protection Commission. within 72 hours of becoming aware of the breach and continue to follow process guided by the DPC as required.

2.7.6 The Data Protection Officer will work with relevant others to complete actions to manage breach and update risk assessments as relevant.

2.7.7 The Data Protection Officer will ensure the Data Breach Notification is updated to include all relevant additional information and that related records are stored in the agreed location.



2.7.8 The Data protection officer will ensure all necessary people are informed of the breech in a timely manner and report to the subcommittee on the board the outcomes of overall data breeches in the organisation on a quarterly basis.

2.8 Making a request for access to Personal Information

2.8.1 KARE will proactively ensure that people have access to their personal information. Any restriction to access to personal information must be in line with FOI and GDPR regulations and this will be communication to the person or their representative.

2.8.2 An individual may make a request to see the information KARE holds in relation to them by using the persons preferred means of communication to ask the relevant Line Manager or to KARE's Data Protection Officer (email dpo@kare.ie)

2.8.3The Data Protection Officer/Designate will acknowledge the request by using the persons preferred means of communication and if necessary, check that the requestor is entitled to receive the information and ask for clarification of the information being requested, including the preferred format for delivery.

2.8.4 The Data Protection Officer will co-ordinate the response to the request. If the request includes sufficient information to process the request the 30-day response period may commence. The Data Protection Officer may consult with the appropriate medical consultant where health information unknown to the person may be harmful or distressing to the individual.

2.8.5 The Data Protection Officer will check the information to be released to ensure that no third-party personal information is disclosed. If necessary, third-party information will be redacted.

2.8.6 Once the information has been collected and a schedule prepared, the Data Protection Officer will contact the requester to finalise arrangements for delivery of the information.

2.8.7 The Data Protection Officer will forward the requested information to the requestor and ensure there is documented confirmation that the information has been received e.g. Registered Post-delivery receipt, confirmation letter.

2.8.8 The Data Protection Officer will maintain a record of the information released to the requestor.

2.9 Procedure for Archiving/Disposing of Documents

2.9.1 Line Manager identifies records to be submitted for Archiving/Disposal on an annual basis Staff member categorises records for paper archive, electronic archive, or disposal

2.9.1 Staff member makes contact with the Archive Administrator to discuss the nature and the quantity of the records to be transferred for paper archiving, electronic archive or disposal and confirm any specific procedures to be followed e.g., the grouping or naming of a collection of records

2.9.2 Staff member prepares records for archiving by putting documents of the same type (e.g., Invoices, Log Sheets, etc.) and in the same date range together as follows:

- Paper archive – in Storage Case issued by the Archive Administrator
- Electronic Archive – in folders or envelopes with
- Disposal (for shredding) – in envelope or box

2.9.3 Staff member will record the details of the documents being submitted to Archive Administrator on an Archive/Disposal of Records Form (electronically) as follows:

a. Name of records in the Storage Case/envelope (e.g., Cash Control, 'Accounts Payable Invoices' or 'Facilities Log Sheets')

b. A date (month and year) of the earliest document in the Storage Case/Envelope

c. A date (month and year) of the latest document in the Storage Case/Envelope.

d. Indicate if the record is for archiving, uploading or shredding

e. Name of staff preparing the records for archiving/disposal

2.9.5 The staff member arranges for delivery of the records to the Archive Administrator

2.9.6 The Archive Administrator receives the documents for archive/disposal and records receipt of the documents on the Archive/Disposal of Records Form.

Note: If the correct procedures are not followed, the records will not be accepted and will be returned immediately, and an email will be sent from the Archive Administrator to the Line Manager. The Archive Administrator will record the Storage Cases/envelopes returned on the Archive/Disposal of Records Form.

2.9.7 The Archive Administrator will arrange for the archive/disposal of records submitted as follows:

I. Records for electronic archiving - schedule documents for scanning and record the date of upload to KARE CID on the Archive/Disposal of Records Form

II. Records for paper archiving - assign Storage Box numbers to the approved Storage Cases, update the Archive/Disposal of Records Form and record the details on the Archive Database Record.

III. Records for disposal - arrange on-site shredding of documents for disposal by an approved Vendor, update the Archive/Disposal of Records Form and record the details on the Archive Database Record as relevant.

2.9.8 The Archive Administrator will store the Archive/Disposal of Records Form as follows:
Service User Records - upload to the service users record on KARE CID under Miscellaneous

Non-Service User Records - upload to KARE connect (Managing the Organisation – Managing Information – Department Documents – Paper Archive – Department)
Non-Service User Records - upload to KARE connect (Managing the Organisation – Managing Information – Department Documents – Paper Archive – Department)

2.9.10 The Archive Administrator will keep a document outlining the archive codes and retention times up to date (titled Archive Codes _Retention Schedule and stored on KARE connect in Managing Information>Open documents)

2.9.11 The Archive Administrator will dispose of documents held in the paper archive when they have exceeded the required retention period.

2.10 Procedures for managing data processing (See Appendix 6)

2.10.1 **Role of data protection officer** (Refer to Appendix 1)

- In Article 38 of GDPR it establishes the position of the DPO, “The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.”
- The DPO is bound by confidentiality in the performance of their tasks. What are the data protection officer roles and responsibilities? - GDPR.eu

2.11 Audit of the policy

- The implementation of this policy will be reviewed on an ongoing basis.
- An audit of its compliance may be conducted in any location at any time.

Appendix 1

Data Protection Officer

KARE's Data Protection Officer:

Sandra Burke

Telephone: 045 448700

E mail: sandra.burke@kare.ie or dpo@kare.ie

Appendix 2

Schedule of Retention Link

Appendix 3 Definitions:

(https://gdpr.eu/)

Data - the personal data (as defined by Data Protection Laws) of others which is shared, stored, used between any parties. The EU's GDPR only applies to personal data, which is any piece of information that relates to an identifiable person.

Data Exporter - shall mean the data controller who transfers the Data.

Data Importer - shall mean the data controller who agrees to receive from the Data Exporter the Data for further processing.

Data Protection Laws - means as applicable the Data Protection Act 2018, the General Data Protection Regulation (EU) 2016/679 (the "GDPR") and any equivalent or replacement law in Ireland, the Electronic Communications Data Protection Directive (2002/58/EC), the ePrivacy Regulations 2011 (SI336 of 2011) and all applicable laws and regulations (including judgements of any relevant court of law) relating to the processing of personal data, direct marketing, electronic communications and privacy including where applicable the formal, binding guidance, opinions, directions, decisions and codes of practice and codes of conduct issued, adopted or approved by the European Commission, the European Data Protection Board, the Office of the Data Protection Commissioner and/or any other applicable supervisory authority or data protection authority from time to time; in each case relating to the processing of personal data;

Regulator - means the Office of the Data Protection Commissioner and/or any other supervisory authority or data protection authority or any other regulator (including a financial regulator) or court; and

Data Processor - A data processor simply processes any data that the data controller gives them.

Data Controller - A data controller is a person, company, or other body that determines the purpose and means of personal data processing (this can be determined alone, or jointly with another person/company/body).

Joint Controller Agreement - Under the General Data Protection Regulation (GDPR), two or more data controllers that jointly decide why and how to process personal data are collectively known as "joint controllers."

Key Activity Owners/system owners – Department responsible for administering the system in KARE.

Stored appropriately – This depends on the type of information and will be determined by that e.g. electronic information may need to be encrypted, Information only stored on KARE ICT in line with use of KARE ICT policy, Hard copy stored in locked filing cabinet.

Process owners – Line manager responsible for managing the overall business process.

Data Processing Agreement - GDPR compliance requires data controllers to sign a data processing agreement with any parties that act as data processors on their behalf. A data processing agreement is a legally binding contract that states the rights and obligations of each party concerning the protection of personal data.

Data privacy impact statement: A Data Protection Impact Assessment (DPIA) is required under the GDPR any time you begin a new project that is likely to involve “a high risk” to other people’s personal information.
Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.
The data privacy impact statement is a summary of the DPIA. It is generally conducted by the DPO for the organization.

In writing - letters, written correspondence including handwritten and electronic formats, including via email.

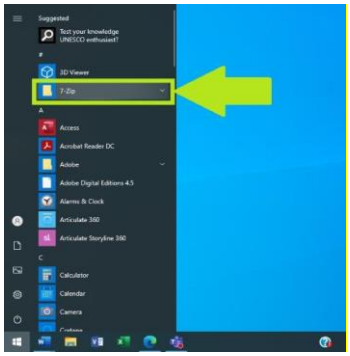
Data processing log – The document that records a comprehensive list of data process activities for the organization.

External audit: An audit from an external party.

Data protection officer - is responsible for overseeing an organization's data protection strategy and implementation. They are the officer that ensures that an organization is complying with the GDPR's requirements.

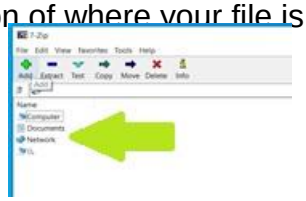
Appendix 4 Sending personal and sensitive information externally via email

- When sending personal and sensitive information externally via email, data shall be attached to the email as a file with password protection. Files shall be password protected using 7-Zip application, to be requested through the ICT department. Examples include information being sent in advance of mental health consultations, review by dietician and other health and wellbeing specialists.
- Images/ Photos are considered personal data under GDPR. Images of individuals being supported by KARE will not be taken without the confirmed consent of the individual or their representative through the service agreement.
- Additional requests outside the service agreement will be done on a case-by-case basis. These will require the individuals consent to their image being taken and the individual must be made aware of the purposes for which the images will be used, by whom, where they will be stored and how long they will be kept for.
- Additionally, individuals have the right to know that they have a right to withdraw their consent to the future use of such photos.
- All personal information being communicated externally will follow the steps detailed below:
- Open the 7zip file manager by selecting the application through the start menu button on your computer

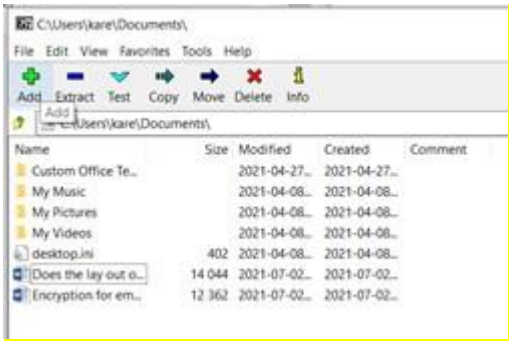


-
-
-
-

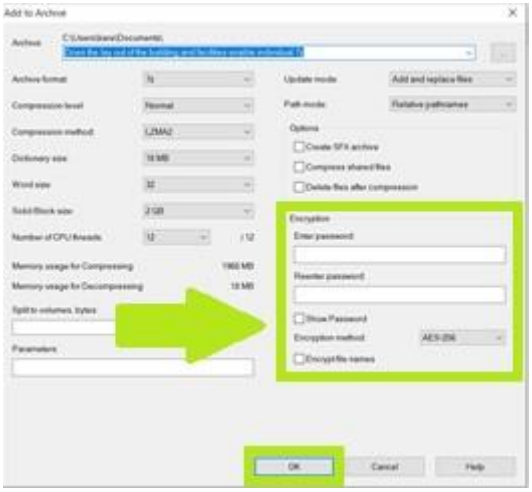
Then select the location of where your file is, i.e. in documents or on computer



- Once you have selected the location, your file should appear on the screen, select file. Press the Green + button below the word ‘file’.



- This will open up a page where you input the password, which will be the service users ID and press ok.



- You then must either send the password by text or phone call to the person receiving the information. **It cannot be sent through the same source i.e., email.**

Appendix 5 Printing personal, sensitive, or confidential information

- If you do print personal, sensitive, or confidential information on a shared printer collect the prints immediately.
- If you find personal, sensitive or confidential information printed on the printer, (store in an envelope) seek to find the owner or shred information.
- This is to be reported as a near miss data breech.
- If there has been an issue with the printed materials not appearing correctly or in the correct location, please cancel the print job.
- Report as a data breach if the printed materials cannot be found.

Appendix 6 Procedures for managing data processing

System access

- Access to necessary ICT systems will be determined and approved by the process owner and administered by the relevant system owner.
- KARE CID account access is automatically assigned in line with the staff members roles and responsibilities. Additional access privileges are requested by the line manager through the KARE CID helpdesk.
- Where requests are made to increase access privileges above standard roles and responsibilities, these will be overseen by the Quality Department as the system owner in consultation with relevant Operational Management Team members or process owner as relevant.

Data Sharing

- Data sharing agreements, data processing agreements, Joint controller agreements, will be completed with external companies where data sharing occurs. They will be drafted by the relevant manager using KARE agreed templates and approved by the Data protection officer. A copy will be stored on KARE connect.

DPIA assessments

- DPIA assessments will be conducted “prior to the processing” of any information and where any new or revised KARE organisational process may require us to gather, store, alter or destroy any personal information.
- It is generally good practice to carry out a DPIA as early as practical in the design of the processing operation (as part of a project or process revision).
- It may not be possible to conduct a DPIA at the very inception of the project, as project goals and some understanding of how the project will operate must be identified before it will be possible to assess the data protection risks involved.
- For some projects the DPIA may need to be a continuous process, and be updated as the project moves forward.
- The fact that a DPIA may need to be updated once processing has actually started is not a valid reason for postponing or not carrying out a DPIA.
- All DPIAs must be conducted by the KARE process owner / project leader using the KARE DPIA template (available on KARE Connect).
- The KARE DPIA template may only be completed by a person who has completed the associated module on HSELanD. In this way all project leaders and process owners should complete the required HSELanD module on ‘Fundamentals of GDPR’ prior to filling out a DPIA.
- The KARE DPO is responsible for reviewing all DPIAs prior to processing of data to ensure appropriate controls are in place.
- Signed off DPIAs by the DPO will be stored by the DPO on KARE Connect and are available upon request.

- Once a DPIA has been completed, the KARE data processing log shall be maintained by the DPO on KARE Connect and is available upon request.

Appendix 7

Archive/Disposal of Records Form

Name of Service User: **KARE ID:**

Department/Service **Date:**

Section 1:

Section A, B, C and D to be completed by Staff Member or Line Manager

Section E, F and G to be completed by Archive Administrator

A. Name of Record	B. Dates of Documents e.g. MarJune 2017	C. Are Documents for Paper Archiving/	D. Name of the Staff preparing Records for archiving	E. Documents Accepted / Rejected by Archive Administrato	F. Signature of Archive Administrator	G. Date on which Documents have been

		uploading or Shredding?		**r**		**accepted or rejected**

_____ _____

Signature of Line of Line Manager **Date**

Section 2: Paper Archiving **To be completed by Archive Administrator**

Box Number	Storage Case Number	Record Name	Master Database updated Y/N	Archive Date

Section 3: Electronic Archiving **To be completed by Archive Administrator**

Name of Record	Folder Location on CID	Date of upload to CID

Section 4: Shredding of Records **To be completed by Archive Administrator**

Name of Record	Date of on-site Shredding