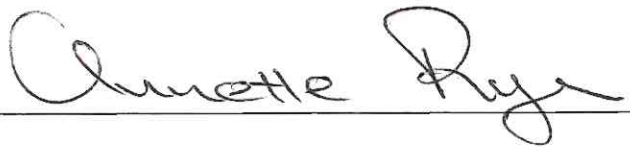
Aurora Kilkenny

Data Retention and Destruction Policy

Policy Number	Policy Developed by	Date Developed
14 – Schedule 5	John Murphy	01.01.2015
Version	**Amendments**	
3	Full review of Policy	
Reviewed by		**Review completed**
Aine Forde		17.07.2024
CEO signature		**Next Review Date**
		17.07.2026

Mission Statement

Enable people with complex needs to experience the same rights as every other citizen and as equal members of the community.

Contents

1.0 Policy Statement

In order to plan for services effectively, to plan for future services and to ensure that a record of services provided is maintained, Aurora Enriching Lives, Enriching Communities must gather and hold information on employees and each person using its services. Information is also gathered and maintained in relation to employees and the designated centres where services are provided.

Aurora will ensure that the Data Retention and Destruction Policy maintains the balance between confidentiality and the obligations of the organisation in relation to the availability of information to the person using services, their families and employees who require access to information in order to do their work.

Aurora complies with the Aurora Data Protection Policy, General Data Protection Regulation (GDPR) and Data Protection Act 2018, the Freedom of Information Act 2014, Aurora Consent & Capacity Policy and the Assisted Decision-Making (Capacity) Act 2015 (ADMC).

Aurora Data Retention and Destruction Policy has been developed in conjunction with the Federation of Voluntary Bodies Guidance on Records Retention, July 2019 and HSE Record Retention Period Policy, 2013.

2.0 Purpose & Scope

2.1. The Data Retention and Destruction Policy has been developed to provide guidance for people and families using services, for employees and for people outside Aurora. The policy is to outline the process for the management of Aurora records throughout the records lifecycle. The activities in this management include the systematic and efficient control of the creation, maintenance and destruction of Aurora records along with the business transactions associated with them.

2.2. The purpose of data and record management is part of Aurora broader function of governance, risk management and compliance. It is primarily concerned with managing the evidence of Aurora activities as well as the reduction or mitigation of risk.

2.3. Elements of Aurora data and record management are as follows:

- Values and Principles in Practice; Access and Confidentiality,
- Description of types of records
- Retention periods for different types of records
- How to file and send records to archiving for safe keeping
- To set out how records are shared with people using services and families
- To set out how employee records are managed
- To describe how other service records are managed

3.0 Guiding Principles

3.1. Confidentiality

Confidentiality requires that at all times records are maintained securely and that information is safeguarded so that only people who need to access this information can do so. The sharing of information is done on the basis of respect and in order to provide Informed Support. This refers to the need for people who support the person/family to have access to information necessary to fulfil their role properly. The same requirement of confidentiality also applies to information about employees.

3.2. Access

Access means that in the first instance information recorded is routinely shared with the person/ family or that they are aware of and can obtain any record about them which they wish to see unless in the rare cases where there are conflicting legal obligations on the Organisation. It means ensuring records are written in such a way as to be easily understood and unnecessary technical language is avoided. Access also means that support is provided for the interpretation of records so that the contents are understood. Good practice means that records will be developed in preferred formats that are accessible for the individual.

3.3. Consent

Each person/family member/employee is fully informed about the type and the content of records which are kept by Aurora through the Privacy Notice. A copy of the current privacy notice is accessible on the website.

In practice, consent is not sought from individuals and families in relation to the collation of personal information by support employees as part of day-to-day service provision. This is because it is legal requirement in order to provide safe services.

However specific consent must be sought in relation to the following instances:

If information is to be used or released for purposes outside of provision of support i.e. photographs and video recording. Aurora's working practices are aligned to the Assisted Decision-Making (Capacity) Act 2015 (ADMC). Circle of Support meetings can facilitate any decision making required. See Aurora Capacity & Consent Policy for further details.

4.0 Function of Records and Files

4.1. The Data Retention and Destruction Policy operates within the legal obligation of the various Acts ensuring we fulfil such obligations. This policy must be read in conjunction with the Data Protection and FOI Policy which covers the following areas:

- Data Protection /General Data Protection Regulation (GDPR)
- Freedom of Information
- Informing People and Families about Records
- Access to Records
- Data Security and Breach Requirements
- Aurora Capacity & Consent

4.2. The primary function of records and files are:

- To meet the legal requirements to which Aurora is subject to necessary to comply with employment and revenue law
- To provide accurate, clear, comprehensive, complete, factual and concise information concerning the condition and support of the person and associated observations.
- To provide a record of progress.
- To ensure information is regularly updated and easily retrieved
- To provide a safe and effective means of communication between members of the employee team
- To provide information to people supported
- To support continuity of supports
- To provide written evidence of supports and service given.
- To record the chronology of events and the reason for any decisions made
- To support quality assessment and audit

4.3. The secondary functions are to provide information for:

- On-going development of services,
- The National Ability Supports System (NASS) which it used by the HSE & HRB (Health Research Board) to gather information about peoples' use and need
- Research purposes, subject to ethical considerations, and
- Responses to requests under the relevant FOI & Data Protection Acts

5.0 Categorisation of Aurora Records and Data

5.1. Types of Data are as follows:

- Emails

- Correspondence
- Documents/Medical and other
- Reports
- Tracking documentation
- Financial statements

5.2 All Aurora functions are responsible for the following in relation to their own data and records:

- Identifying – what information must be retained for compliance
- Categorising – dividing records into relevant file systems
- Storing – ensuring data and records are kept safely and securely
- Maintaining – ensuring data and records are kept accurate and up to date
- Archiving – ensuring archiving in line with archiving pathway (Appendix 1)

5.3 Records can be categorised as either related to:

- Aurora as a service provider
- Aurora Governance records
- Financial management, insurance and legal records
- Registered designated centres
- People using Aurora services
- Aurora employees
- Families
- Stakeholders/suppliers/contractors

6.0 Security, storage and access to Aurora Records and Data

6.1. Aurora will ensure that there are appropriate security/provision levels in place for all records and access to these records is based on a need for such information. Further to Aurora Data Protection and Communication Policies, employees must not access work emails on any personal devices. Breach of these policies may result in disciplinary action.

6.2. Employees will not disclose information or provide access to records to anyone who is not authorized to have such access.

6.3. Freedom of information and data access request will be dealt with in accordance with the relevant legislation and Aurora polices.

6.4. Employees will maintain and store records in accordance with agreed processes and procedures.

6.5. Employees will ensure that they move records from any temporary storage arrangements, such as temporary files etc. into the relevant record management system at the earliest possible opportunity.

6.6. Non electronic records will be kept in suitable storage conditions that ensure they are protected from damage and/or loss.

6.7. Line Managers will ensure electronic records are stored appropriately in Aurora systems.

6.8. Any processing of data and records is tracked and logged, including cross function movement (file removal form). All information belonging to people supported is retained, stored and destroyed in line with legislative and regulatory guidelines.

6.9. Any email that is typed up relating to a person supported must be copied to the person for their information/file.

6.10 In the event of a lost file, it should be reported to the Data Protection Officer via the Data Breech Form immediately the loss has been identified.

7.0 Record Retention Periods

7.1. Aurora has adopted the HSE Record Retention Periods Health Service Policy 2013. All retention periods can be accessed for review within the above-named policy on Aurora Q drive (see pages 5 to 71).

8.0 Archiving and destruction of data and records

8.1. Aurora maintains a central archive where all data and records are held.

8.2. Each designated centre stores a house specific archive which holds all medical data and records for each person supported

8.3. Aurora records should be held locally for one year (excepting person's medical information) then archived followed the Aurora archiving pathway (Appendix 1) and following the above-mentioned retention periods.

8.4. Aurora will ensure that there are clear retention periods and methods of destruction for all record types in line with relevant regulations and legislation. The document of retention periods is held on Aurora Q drive and with the Compliance and Governance Manager.

8.5. Aurora Line Managers identify records to be submitted for archiving/destruction on an annual basis in line with Aurora archiving Pathway (Appendix 1).

8.6. Line Managers ensure that the File Archiving and Shredding form is completed documenting the archiving and/or destruction of data and records (Appendix 2)

8.7. Records are destroyed after a period of 20 years once a person has ceased receiving services and after 8 years if the person dies. Record Management is responsible for the retention of these records.

8.8. In Aurora, records that reach their retention period are destroyed by a recycling company by means of confidential shredding.

8.9. Aurora will ensure that these records are then placed in recycling bags and collected by the recycling company. The date of destruction is recorded on the certificates issued by the recycling company and stored in the Aurora Finance Department.

8.10. Where employee records have reached the timeframe for removal from the house, the line manager should contact the HR department for advice on how to proceed. PICs should ensure the safe transit to Danville and keep a record in their diary of the information that was sent for shredding, the person responsible in charge at the time and the date.

8.11. Each employee must complete GDPR training on HSELand.ie. Line Managers are responsible for ensuring that all their staff receives GDPR training.

8.12. On completion, the certificate of achievement must be forwarded to the Training Department for recording purposes.

8.13. In addition, the Data Protection Officer will brief employees on this policy as part of their induction to the organisation.

8.14. The Data Protection Officer will be available to you to answer any queries regarding this policy and training options available to you.

9.0 Archiving of Closed Records belonging to people supported

9.1. Closed Files are defined as records that relate to any person who no longer receives a service from Aurora. When a person exits Aurora or dies, their records are closed off and archived. Records must be retained in the service for a period of 8 years after a person supported has died or left the service. Compliance & Governance Manager will be notified of any file closure by email or Change of Status Form when a person dies or transfers from Aurora.

9.2. When a person supported dies, Compliance & Governance Manager will write to all those involved with the particular person supported advising that all records relating to that person be returned to archiving within two weeks so the records can be updated before the file is closed. The file will then be closed and as per procedure above.

9.3. Where the person supported attends a HIQA Designated Service the person's records will remain within Aurora for a further for 7 years.

10.0 Archiving of Staff Records and Location Specific Information

10.1. All records retained during their specified periods are traceable and retrievable. Any file movement, use or access is tracked and logged, including inter-departmental changes. All company and employee information is retained, stored and destroyed in line with legislative and regulatory guidelines.

11.0 Best Practice in Records Management

11.1. Keeping a Clear Desk. Staff should never leave personal or sensitive information on their desks unattended or in any area that it may be seen or accessed by an unauthorised person. At the end of each day staff must lock away all personal and sensitive information.

11.2. Saving Electronic Records. When you are saving electronic records follow correct file routing path. A guidance document to explain this process is available with this policy. Implementing this practice ensures that records can be located and retrieved in a timely fashion. It also reduces the proliferation of duplicate copies of documents and will help when it comes to archiving paper records.

11.3. Printing to the Photocopier Documents will be held in the memory of the machine and can only be printed as and when you enter your password into the printer ensuring confidential documents are not left lying around for everyone to access.

12.0 Communicating externally through E-mail.

12.1. For security reasons employees must not forward their Aurora email messages to their own personal email account.

12.2. Emails can be retrieved, examined, and used in a court of law. Information on people supported can only be externally transferred electronically if the file (attachment) is password protected. The password used to read the attachment must not be sent along with the original e-mail message.

12.3. Once you have sent the password protected document you will need to remove the password from the actual document. This is important as the document may need to be accessed at a later date.

12.4. The body of the e-mail should not contain any identifiable information either that could potentially identify a person supported.

13.0 Removing Records from On-site

13.1. Employees must not remove any confidential information (irrespective of format) from the facility they are employed at without the authorisation of their line

manager. Such authorisation must be issued in advance and may apply thereafter if necessary. Where an employee has been authorised to remove confidential or restricted information from an Aurora office or location, they will be responsible for the safe transport and storage of the information i.e. locked in the boot of your car during transit and in locked storage when not in use. Employees should also remember to complete Aurora File Removal Form (Appendix 3).

14.0 Appendix 1 – Archiving Pathway

Aurora Archiving Pathway

- All data and records (files) belonging to people supported are stored safely and securely in the designated centre and contain current and previous year. i.e. in 2022, records belonging to the person supported should contain data from 2022 and 2021.

- Data and records from previous year(s) must be archived with the exception of medical data i.e., in 2022, data from 2020 and previous years must be archived

- All files to be arranged in chronological order i.e. filed in date order.

- Files will only be accepted in a respectful manner i.e., chronological order, no pages falling out or pulled out, not overfilled etc

- Please ensure all records are stored securely and with integrity as per GDPR 2018.

- While preparing for archiving, all recording forms should be filed in an orange file with same index per the persons recording sheets.

- **Medical File**
    - All medical data and recordings for the previous five years should be held on the current medical file.
    - Any medical data prior to this will be filed in the archived medical file which will be stored in the designated centre that the named person resides in (this record (file) should transfer with the person to wherever they reside).
    - This medical archived record (file) is a duplicate of the current medical file and all details relating to medical appointments, hospital appointments or any information pertaining to the health of the person should be stored on this file for easy access in the event of researching medical history.

- Data and records identified for archiving should be transferred safely and securely to Aurora archive having completed the Log for Archiving, Scanning and Shredding.

- Contact Compliance & Governance Manager if in need of assistance.

15.0 Appendix 2 – Archiving, Shredding and Scanning of Files

Aurora

LOG FOR ARCHIVING, SCANNING AND SHREDDING OF FILES:

Function : ..... **Date:** .....

Date:	File Description:	Received by:	Received from:	Date Scanned and Filed to System	Date of shredding of File:	Signed off by:

Under Articles 5 & 9 of the GDPR, Aurora has lawful purpose for the processing of personal data (name, and sensitive data (health matters) of people supported for internal communications. For external communications, unique identifier numbers (NAC) are to be used as opposed to names. All employees are subject to the confidentiality clause in their contracts of employment

16.0 Appendix 3 – File Removal Form

File Removal Form

The movement of these documents/files/folders to be tracked :

Personal File	*Stock Check Book*
Medical File	*Prescription sheets*
Kardex	*House Folders*
Archiving Folders	

Aurora
Enriching Lives,
Enriching Communities

Address:

Document/File/Folder Name	Reason for Removal from House	Date Removed	Person Removing	Date Returned	Person Returning

Directions for filing this document while active: **Handover Folder**
Directions for filing this document when completed: **Handover Archive File**