Aurora

Enriching lives, Enriching Communities

Confidentiality Policy

Policy Number	Policy Developed by	Date Developed
04 – Other Policies	John Murphy Geri Wilson & Áine Forde	01.01.2015 18.11.2020
Version	**Amendments**	
3	Change in terminology from: Staff to employee SPC to Aurora 8.0 Inclusion of Breach of Confidentiality point	
Reviewed by		**Review completed**
HR Manager		24.06.2024
CEO signature		**Next Review Date**
Annette Ryan		24.06.2026.

Mission Statement

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

Table of Contents

1.0 Introduction

1.1 The purpose of this Policy is to provide clear guidelines for all employees of Aurora Kilkenny in relation to Aurora's obligations in maintaining the confidentiality of all personal information held for all people supported.

2.0 Scope of the Policy

2.1 This policy relates to all employees, including agency workers, clinicians, volunteers, students and anyone involved in the provision of services in Aurora.

2.2 A copy of the written policy on confidentiality should be made available to all employees, including temporary/relief employees or agency workers.

2.3 It is the responsibility of managers to ensure that all employees including temporary employees are made aware of Aurora's confidentiality policy and that all employees read and sign the confidentiality declaration. Appendix 1

3.0 Principles of Confidentiality

Confidentiality is underpinned by a number of principles:

3.1 Minimum necessary personal information:

Use anonymized information if it is practicable to do so and if it will suit the purpose.

3.2 Management and protection of information:

Ensure that all information held or controlled by Aurora is effectively protected at all times from improper access, disclosure or loss.

3.3 Awareness of responsibilities.

Maintain an awareness of the information governance appropriate to the role.

3.4 Compliance with the law

All employees must be satisfied that they are handling personal information within the relevant laws i.e. GDPR and Data Protection Act 2018and be aware of their responsibilities when doing so.

3.5 Access to identifiable information should be on a strict need-to-know basis

Only those employees who need access to identifiable information should have access to it and they should only have access to the information items that the need to see.

3.6 Consent & supported persons' entitlement to access their information.

Respect and assist persons supported to exercise their rights to be informed about how their personal information will be used.

4.0 Disclosure of Information

Confidentiality is an important legal and ethical duty but it is not an absolute right.

4.1 Personal information about persons supported can be disclosed when any of the following applies:

4.1.1 The person supported consents explicitly or implicitly either for their own care, or for local clinical audit.

4.1.2 The disclosure is given in good faith and for the overall benefit of the person supported who may lack capacity to consent at that time

4.1.3 If there is a legal bases for sharing the personal and sensitive information belonging to a person supported

4.2 When disclosing information about a person supported you must:

4.2.1 Use anonymized information if practicable,

4.2.2 Be satisfied that the person supported has ready access to information explaining how their personal information will be used

4.2.3 Follow all relevant legal requirements,

4.2.4 Keep disclosures to the minimum necessary for the purpose,

4.2.5 Keep a record of your decisions and actions.

4.3 Disclosing Information for Direct care

4.3.1 Appropriate information sharing is an important element of the provision of safe and effective care of persons supported.

4.3.2 Persons supported may be put at risk if those providing care do not have access to relevant, accurate and up to date information.

4.3.3 Multi-disciplinary and interagency teamwork is also an integral part of care and information sharing is central to this, provided it is shared within the framework of ethics and law.

4.4 Disclosing Information for Secondary Purposes

4.4.1 Many important uses of persons' supported information contribute to the overall delivery of health and social care.

4.4.2 Examples include health service management, research, epidemiology, public health, education and training.

4.4.3 This information is vital to ensure that the health and social care system can plan, develop, conduct research and be publicly accountable for the services it provides.

5.0 Consent

5.1 The usual basis for sharing information about persons supported is the consent of the person supported, whether that is explicit or implicit.

5.2 You may rely on implicit consent in the provision of direct care if the following criteria are met:

5.2.1 You are accessing the information to provide or support the persons supported direct care or are satisfied that the person with whom you are sharing the information is receiving it for the same purpose.

5.2.2 The information is readily available to the person supported and is tailored to their individual communication requirements, i.e. pictures,

5.2.3 The person with whom the information is shared is aware of the requirements in respect of keeping the information confidential.

5.3 Disclosing information when a person supported lacks capacity to consent

5.3.1 You must work on the presumption that every adult has the capacity to make decisions for themselves, unless proven to the contrary.

5.3.2 You must not assume that a person lacks consent because of their age, disability, medical condition or apparent inability to communicate.

5.3.3 You must assess the person's capacity to make a particular decision at the time it needs to be made, acknowledging that fluctuations in a person's condition may affect their capacity to process information and communicate their wishes.

5.3.4 When making the decision to disclose information about a person supported who may lack capacity you must:

5.3.4.1 Ensure that the person supported is at the center of any

decision made

5.3.4.2 Respect the dignity and privacy of the person supported

5.3.4.3 Consider the views of people close to the person supported and the views of those who support the person, i.e. key employee team

5.3.5 You may need to share personal information with a person's supported family to enable you to access the overall benefit of the person, but that does not mean that they have a general right of access to information.

5.3.6 You must share relevant information with anyone who is authorized to make health and welfare decisions on behalf of the person supported, i.e. a person appointed by a Court- Ward of Court or Decision-Making Representative

6.0 Managing and Protecting Personal Information

6.1 All employees must ensure that the records they are responsible for are recorded, stored, transferred, protected and disposed of in line with data protection law and any other relevant policy.

6.2 All employees must have an awareness of the governance of information appropriate to their role.

6.3 Managers must ensure that the employees they manage are trained and understand their information governance responsibilities.

6.4 It is the responsibility of employees to ensure that any personal information that is held is secure

6.5 Employees must not access the personal information about a person supported unless there is a legitimate reason to do so

6.6 Employees must not share personal information about persons supported where others can overhear it

6.7 Human Resource employees who are responsible for employment contacts must ensure that they contain obligations to protect confidentiality and are in line with data protection law.

6.8 Guidance on the retention of records is contained in Aurora's Data Retention and Destruction Policy.

6.9 All records including financial, medical, support plans, human resources, complaints etc. must be kept securely, accurate and up to date.

6.10 Health and social care records can include but are not limited to:

6.10.1 Handwritten notes

6.10.2 Electronic records

6.10.3 Correspondence between clinicians

6.10.4 Reports, i.e. psychology, psychiatric, physiotherapy.

7.0 Processing information in line with Data Protection Law

7.1 The Data Protection Act 2018 sets out the responsibilities of data controllers when processing personal data.

7.2 As a data controller, we must be aware of and meet our obligations under data protection law. This includes the responsibility to ensure that the personal and sensitive information of a person supported is handled in ways that are transparent and that the appropriate organisational measures are in place to guard against data loss.

7.3 You must ensure that information is readily available to all persons supported if requested. All employees must be aware of the confidentiality, data protection and record management policies and procedures of Aurora and how to raise concerns if appropriate. This includes policies on the use of laptops and mobile phones.

8.0 Breach of Confidentiality

Any actual or alleged breach of confidentiality by an Aurora employee is a breach of policy and may result in remedial and/or disciplinary action.

9.0 Relevant Legislation/Policy

- Data Protection Act 2018
- GDPR 2018
- Aurora Contract of Employment
- Assisted Decision-Making Act 2015
- HSE National Consent Policy
- Aurora Capacity & Consent Policy
- Freedom of Information Act 2014
- Aurora Retention & Destruction Policy 2022
- Aurora Mobile Phone Policy
- Aurora Internet Acceptable Use Policy