Aurora

Confidentiality Policy

Policy Reference:	*AQ8*
Version Number:	*2*
Applies to:	All services
Associated documents:	*GDPR* *Child Protection Policy* *Adult Safeguarding Policy*
Approved by:	*Quality Assurance Director*
Implementation date:	*March 2021*
Next review due by:	*March 2024*

1. Introduction

1.1 Purpose

To provide clear, unambiguous guidance to the legal and professional expectations in handling information which is considered confidential to the business and to ensure good practice throughout the organisation.

1.2 Legal Framework

This Policy fulfils the requirements of:

Keeping Children Safe in Education

Working Together to safeguard children

Data Protection Act

(please refer to the most recent versions)

2. Scope

This policy relates to information which is related to The Aurora Group's business. Information relating to how we manage personal data regarding the children and young people we work with is found in our Child Protection Policy, our Adult Safeguarding policy and our GDPR policy.

3. Duty not to disclose confidential information

All employees will at some point have access to information which is confidential. Employees must not disclose any confidential information to anyone who is not an employee of the Aurora Group without specific permission.

Where employees have access to information which is confidential even within the Aurora Group (such as payroll details), they must not disclose it to anyone who is not authorised to access that information.

4. What information is to be treated as confidential?

Any information which you have access to by virtue of being an employee of the Aurora Group, and which is not in the public domain, is to be considered confidential. This includes, but is not limited to:

- Information about stakeholders or clients, their affairs or dealings with the Aurora Group
- Information which could potentially damage the Aurora Group, its brand or reputation, any employee or officer of the Aurora Group, or any person or organisation associated with the Aurora Group
- Information which is labelled as private or confidential
- Information which is not generally known to the Aurora Group's competitors
- Technical details or specifications relating to any of the Aurora Group's products or services
- Information relating to the Aurora Group's plans or strategic direction, finances or performance, or market research undertaken by the Aurora Group
- Information which relates to any of the Aurora Group's business deals or arrangements

5. Managing confidential information:

Confidential information may be disclosed in a number of ways, for example, during face-to-face conversations, over the telephone, by fax, by email, through social media, during virtual meetings, or over the internet. Action should be taken to ensure confidential information is not shared without authorization. Actions include, but are not limited to ensuring that:

- confidential documentation is not visible to others or left unattended and is stored securely
- Any calls, conversations or meetings (including virtual meetings) regarding staff or students must be undertaken in an environment which retains confidentiality.

6. Consequences of breaching confidentiality

Where an employee commits any disclosure of confidential information in breach of this policy, this disclosure will be addressed through the disciplinary policy and in most cases will be treated as gross misconduct.

7. Roles & Responsibilities

Site Level and Central Senior Leadership Teams

- Ensure employees fully understand the policy
- Act appropriately if procedures are not being followed

All staff

- Comply with the policy as outlined above
- Use internal systems to raise concerns where appropriate
- Report all safeguarding concerns as per local policy

8. Implementation

All site senior leadership teams and Central Function leads are responsible for ensuring this policy is implemented in their site or function

9. Support, Advice and Communication

More support advice and guidance can be provided by the Site or function lead. Questions concerning data protection can be addressed to the quality and governance administrator. At sites, the Operations Directors can provide operational support and further information regarding regulatory expectations.

10. Review

This policy will be reviewed every 3 years by the policy owner and ratified by the Executive Team.