Confidentiality Policy

Sept 2021

Version 4

1. Scope

All employees of Expanse Learning, including board members, investors, contractors and volunteers, who may have witnessed or have access to confidential information.

2. Policy Brief & Purpose

Expanse Learning have designed the Confidentiality Policy to explain how we expect our employees to treat confidential information and actions. Employees will unavoidably receive, witness actions and handle personal and private information about students and service users. We want to make sure that this information is handled and dealt with in an appropriate manner.

We must protect this information as it may:

- Be legally binding *(e.g. sensitive data)*
- Be a Safeguarding concern *(must be reported to the relevant Safeguarding Lead (SGL) – refer to Safeguarding Policy)*
- Be able to protect the dignity and well-being of our client group,

3. Policy Elements

Confidential and proprietary information is secret, as well as information in accordance with the Data Protection Act (2018) that applies to personal data held in both electronic and paper form and is designed to strengthen the right to privacy of the individual by ensuring that the processing of personal data is done in accordance with the principles of the DPA and General Data Protection Regulations (2018).

All actions of students and service users that may be seen as unsafe or actions that would be deemed dangerous must be reported to line managers or safeguarding leads within your respective sites through the relevant DatabridgeMIS event. Due to the nature of what the incident could be classed as you are prohibited to communicate any of this information outside of the organisation and peers unless instructed by any of the above named.

Employees may have various levels of authorised access to confidential information and witness a number of acts by our client group.

What employees ***should*** do:

- Adhere to any relevant policies:

ELGR-POL-DPM-004 - Clear Desk and Clear Screen Policy
ELGR-POL-DPM-005 – Data Management Policy
ELGR-POL-DPM - Data Sharing Policy
ELGR-POL-ICT-001 - ICT Acceptable use Policy
ELGR-POL-HRM-001 - Staff Code of Conduct Policy
ELGR-POL-DPM-002 - Data Protection and Privacy Notice

- Lock or secure confidential information at all times
- Make sure they only view confidential information on secure devices
- Only disclose information to other employees when it's necessary and authorised
- Keep confidential documents inside our company's premises unless it's absolutely necessary to move them and agreed by their Line Manager or SLT.

What employees ***shouldn't*** do:

- Use confidential information for any personal benefit or profit,
- Disclose confidential information to anyone outside of our company,
- Talk about students and service users to anyone outside of the company structure.
- Replicate confidential documents and files and store them on insecure devices or location,
- Not discuss what they have witnessed unless in team meetings or if reported to their Line Manager or SGL.

(This is to help protect the dignity and respect of Expanse Groups students and service users)

When employees stop working for our company, they're obliged to return any confidential files, and are still bound by confidentiality not to discuss students and service users' happenings during their time with Expanse Learning.

4. Good Practise

- During team meetings bring any concerns to the team to discuss *(if unsure of course of action)*
- Not discussing Students and service users to anyone outside of the organisation in any capacity including family and friends

- It is down to each staff member to be aware of the SGL for their provision *(This will be covered during stage 3 of the Induction Process – refer to **"ELGR-HR-003(v3) - Induction Policy"**)*
- When communicating information concerning students, in any manner, it is your responsibility to ensure that their personal dignity, confidentiality, and personal well-being, is taken into account and maintained at all times.

5. Confidentiality Measures

Expanse Learning have measures to ensure that confidential information is well protected through:

- The safe storage and security paper documents
- Encrypting electronic information and safeguard databases (See appendix A)
- Ensuring employees sign a declaration of confidentiality (Completed during Stage 2 of the "Induction Process")

6. Exceptions

Confidential information may occasionally have to be disclosed for legitimate reasons for example:

- If a regulatory body requests it as part of an investigation or audit
- If our company examines a venture or partnership that requires disclosing some information *(within legal boundaries)*

7. Disciplinary Consequences

- Employees who don't respect our confidentiality policy will face disciplinary and, possibly, legal action.
- We'll investigate every breach of this policy and as such, Expanse Learning may terminate any employee who wilfully or regularly breaches our confidentiality guidelines.
- This policy is binding even after separation of employment.

8. Ensuring the Effectiveness of the Policy

All staff will receive a copy of the confidentiality policy through DatabridgeMIS. New employees will be introduced to the confidentiality policy via induction and training.

9. Monitoring and Review

The policy will be reviewed annually in line with any changes and new guidance, amendments will be proposed and agreed by the Board of Directors.

Impact of non-compliance

Staff:	Disciplinary action, Support, Action Plan
Student:	Not applicable
Legislation/organisational:	statutory and non-regulated compliance. Prosecution, Staff Retention, Poor employee performance etc
Compliance lead:	Corporate Services (Human Resources)
Policy Reference:	ELGR-POL-HRM-012
Version:	4
Agreed policy location:	DatabridgeMIS
Does the policy require Governor approval?	No

Approval

Prepared by	***Approved by***	***Counter Signatory***
Scott Roberts	Tony Brown	Karl Wane
01/09/2021	01/09/2021	01/09/2021
		
Head of Corporate Services	CEO	Director of College

Version Control

Version	***Date***	***Revision***	***Review Date***
1	17/07/2018	First Issue	31/08/2019
2	14/08/2019	Policy Reviewed	31/09/2020
3	01/09/2020	Policy Review and transfer to new template. Policy amended to include Databridge references and links to relevant policies.	31/08/2021
4	01/09/2021	Policy Reviewed	31/08/2022
5			

Appendix A – Types of encryptions

Kinds of Content	Encryption Technologies
Files on a device. These files can include email messages saved in a folder, Office documents saved on a computer, tablet, or phone, or data saved to the Microsoft cloud.	BitLocker in Microsoft datacenters. BitLocker can also be used on client machines, such as Windows computers and tablets Distributed Key Manager (DKM) in Microsoft datacenters Customer Key for Microsoft 365
Files in transit between users. These files can include Office documents or SharePoint list items shared between users.	TLS for files in transit
Email in transit between recipients. This email includes email hosted by Exchange Online.	Office 365 Message Encryption with Azure Rights Management, S/MIME, and TLS for email in transit
Chats, messages, and files in transit between recipients using Microsoft Teams.	Teams uses TLS and MTLS to encrypt instant messages. Media traffic is encrypted using Secure RTP (SRTP). Teams uses FIPS (Federal Information Processing Standard) compliant algorithms for encryption key exchanges.