Policy Name	**INFORMATION ASSURANCE**
Relevant To	**Federation ☒** **Bidwell Brook Only ☐** **Ellen Tinkham Only ☐**
Type of Policy	**Model ☒** **School ☐**
Name of Policy Holder	**Christine Walker**
Subject/Department	**Communications / GDPR**
Approved By	**Full Governing Body ☐** **CBT Governors ☒** **T&L Governors ☐** **SLT ☐**
Version Date (if applicable)	**n/a**
Date of Last Review	**Summer Term 2025**
Date of Next Review	**Summer Term 2026**

1. Introduction

1.1 Information is a major asset that the Learn to Live Federation has a duty and responsibility to protect. The Federation shall manage its security risks effectively, collectively and proportionately to achieve secure and confident working environments.

1.2 The purpose of this Information Assurance Policy is to set out a framework for the identification, monitoring and management of information risks. This policy seeks to protect the Federation's information assets from all threats, whether internal or external, deliberate or accidental to ensure business continuity and minimise business damage to enable the Federation to deliver its strategic and operational objectives.

1.3 This policy is a key component of the Federation's overall information security management framework and should be considered alongside the Data Protection Policy.

1.4 The objectives of this policy are to preserve:

Confidentiality – Access to data shall be confined to those with appropriate authority.

Integrity – Information shall be complete and accurate. All systems, assets and networks shall operate correctly, according to specification.

Availability – Information shall be available and delivered to the right person, at the time when it is needed.

1.5 In addition, this policy aims to establish and maintain the security and confidentiality of information, information systems, applications and networks owned or held by the Federation by:

- Ensuring that all members of staff are aware of and fully comply with the relevant legislation as described in this or other policies.
- Describing the principles of security and explaining how they shall be implemented in the organisation.
- Introducing a consistent approach to security, ensuring that all members of staff fully understand their own responsibilities.
- Creating and maintaining within each school a level of awareness of the need for Information Security as an integral part of day to day business.
- Protecting information assets under the control of the Federation.

2. Scope

2.1 This policy outlines the framework for the management of Information Security within the Federation. It applies to all employees, agency and temporary staff, contractors, Governors and third parties, who have access to information systems or information used for Federation purposes. Where this policy reads "staff", it should be read to include all the entities in paragraph 2.1.

2.2 Information takes many forms and includes (but is not limited to):

- Hard copy data printed or written on paper;
- Data stored electronically;

- Communications sent by post/courier or using electronic means;
- Stored tape, microfiche, video, DVD, CD;
- Speech.

2.3 This policy continues to apply to staff even after their relationship with the Federation ends.

3. Legislation

3.1 The Learn to Live Federation is obliged to abide by all relevant UK and European Union legislation. The requirement to comply with this legislation shall be devolved to staff who may be held personally accountable for any breaches of information security for which they may be held responsible.

3.2 The Federation shall comply with the following legislation and other legislation as appropriate:

- Computer Misuse Act 1990
- Copyright Designs and Patents Act 1988
- Environmental Information Regulations 2004
- Equality Act 2010
- Freedom of Information Act 2000
- Human Rights Act 1998
- Local Government Act 1972
- Local Government Act 2000
- Regulation of Investigatory Powers Act 2016
- Re-use of Public Sector Information Regulations 2005

3.3 The design, operation, use and management of information systems must take into account applicable legislation, regulations, security best practice and contractual security requirements.

4. Breach of Policy

4.1 All reckless or deliberate breaches of this policy will be investigated and may be referred to the HR Department who will consider whether disciplinary action should be taken against the member of staff concerned. Alleged breaches of this policy will also be investigated by the Data Protection Officer as an information security incident and may also be referred to HR and Senior Leadership as considered necessary.

5. Policy Review

5.1 This policy will be reviewed by the Data Protection Link Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Link Officer, Christine Walker, christine.walker@learntolivefederation.co.uk

6. Security Policy Framework

6.1 Responsibilities

6.1.1 Senior Information Risk Owner - The Executive Head has overall responsibility for ensuring there is appropriate technical and organisational security in place to protect the Federation's information assets and shall seek regular assurances from key staff that these measures are effective.

6.1.2 Technical & Information Security - Operational responsibility for technical security rests and information security rests with the Federation ICT Manager who is responsible for implementing, monitoring, documenting and communicating security requirements for the organisation, and keeping the Executive Head notified of the effectiveness of the Federation's security measures.

6.1.3 Line Managers - Line managers are responsible for ensuring that their permanent and temporary staff and contractors are aware of the information security procedures applicable in their work areas; their personal responsibilities for information security and how to access advice on information security matters. Line managers are individually responsible for the security of their physical environments (for example offices) where information they are responsible for is processed or stored.

6.1.4 All staff - All staff are personally responsible for complying with the Federation's Data Protection Policy. All staff must ensure the information they have access to, handle and share or permit access to, is lawful, securely and professionally handled at all times.

6.2 Information Assets

6.2.1 All information assets shall be accounted for and recorded on the Schools Information Asset Register (IAR). Each asset will have an identified Information Asset Owner and an Information Asset Administrator who shall be responsible for ensuring there is appropriate security in place to protect their information assets.

6.3 Culture, education and awareness

6.3.1 An ongoing security awareness programme shall be established and maintained to ensure that staff are aware of security procedures and understand their personal responsibilities for safeguarding assets and the potential consequences of breaching security rules. This programme will be developed and managed by the Federation ICT Manager.

6.3.2 Information security awareness training shall be included in the staff induction process.

6.4 Information security incident management

6.4.1 Information security incidents shall be reported, recorded on CPOMs and investigated. Mitigating actions shall be taken to prevent incidents reoccurring. The Data Protection Link Officer will be responsible for the management of all information security incidents and will regularly report on trends, risks and mitigations to the Executive Head as required.

6.5 Information risk monitoring and ownership

6.5.1 The Data Protection Officer will monitor information risks identified during the course of conducting security incident investigations, risk assessments or through direct engagement with services. Information risks are to be recorded on CPOMs.

6.5.2 The Data Protection Link Officer will classify all information risks according to the following risk stratification matrix, with ownership assigned to the relevant management.

Risk classification	Description	Risk owner
Low risk	The confidentiality, availability or integrity of the School's information has been adversely affected. However, the impact on the School is negligible.	Direct report to relevant Head of Site via CPOMs
Medium risk	The confidentiality, availability or integrity of the School's information has been significantly affected such that there is a measurable impact on the School.	Head of Site/ Executive Head
High risk	The confidentiality, availability or integrity of the School's information has been significantly impacted to such an extent that there are significant business continuity risks, reputational risks or risk of regulatory action.	Executive Head/ Data Protection Officer

6.6 Accreditation of ICT systems

6.6.1 All relevant ICT systems that handle, store and process sensitive information or business critical data, or are interconnected to cross-government networks or services (eg Wonde), will be risk assessed to identify and understand the relevant technical risks and subject to an annual (or other specified timeframe) accreditation by the Federation ICT Manager.

6.7 Physical Security

6.7.1 The Federation will implement proportionate physical security controls to prevent unauthorised access to locations where paper-based assets and ICT systems are stored and safeguard information from theft, criminal damage, natural hazards and national security threats. Critical or sensitive information processing facilities will be housed in secure areas protected by security perimeters with appropriate security barriers and/or entry controls.

6.8 Personnel Security

6.8.1 The Federation shall have appropriate personnel security in place to provide assurance as to the trustworthiness, integrity and reliability of its employees. The Federation will apply His Majesty's Government (HMG) recruitment controls described in the Baseline Personnel Security Standard, where required.

6.9 Access Control

6.9.1 Access to information and information systems by staff shall be granted according to role and business requirements and only to a level that will allow them to carry out their duties.

6.10 Technical security

6.10.1 The Federation shall have appropriate technical measures and security controls in place to protect its network from threats and attacks that seek to compromise the confidentiality, integrity and availability of the Federation's information.

6.11 Privacy Impact Assessments and Information Risk Assessments

6.11.1 Article 29 of the GDPR creates a statutory obligation on Devon County Maintained Schools to ensure that a privacy impact assessment is undertaken on all new systems, processes or procedures that intend to process personal data, prior to their implementation. Such assessments are to be carried out by or in consultation with the Data Protection Link Officer.

6.11.2 An information risk assessment will be conducted on any information asset or system where a vulnerability has been identified. This may be in response to a security incident investigation or following advice from the Data Protection Officer.

6.12 Business Continuity and Disaster Recovery Management

6.12.1 Arrangements shall be in place to protect critical business processes from the effects of failure or disasters and to ensure the timely resumption of business information systems. Business continuity and disaster recovery plans shall be in place for mission critical information, applications, systems and networks and tested regularly.

6.13 Freedom of Information Act & Data Protection Act requests

6.13.1 The Federation's information and records shall be stored in a manner which facilitates its timely and secure retrieval to enable the Federation to respond to requests for information and fulfil its obligations under the Freedom of Information Act and Data Protection Act. Policies and procedures shall be in place to manage these requests and adhered to by all staff. This policy may be disclosed under the Freedom of Information Act 2000 upon request, subject to any exemptions.

7. Policy History

7.1 This Policy is maintained by the Data Protection Link Officer and will be reviewed on an annual basis. For help in interpreting this policy, contact the Data Protection Link Officer, Christine Walker christine.walker@learntolivefederation.co.uk

Policy Date	Summary of Change
01/05/2018	New policy created
03/07/2024	Edited for clarity and amended hyperlinks