Version	June 18
Owner	
Adopted	June 18
Last Reviewed	
Review Cycle	3 years
Next Review	June 2021

Information Assurance Policy

1. Introduction

1.1 Information is a major asset that The Topsham School (the School) has a duty and responsibility to protect. The School shall manage its security risks effectively, collectively and proportionately to achieve a secure and confident working environment.

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 School's information assets from all threats, whether internal or external, deliberate or accidental to ensure business continuity and minimise business damage to enable the School to deliver its strategic and operational objectives.

1.3 This policy is a key component of the School's overall information security management framework and should be considered alongside the Data Protection Policy, Security Incident Management Policy and Procedure.

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 School 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 the 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 School.

2. Scope

2.1 This policy outlines the framework for the management of Information Security within the School. It applies to all School employees, agency and temporary staff, contractors, Governors and third parties, who have access to information systems or information used for School 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 School ends.

3. Legislation

3.1 The School 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 School 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 Human Resources 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 in accordance with the Security Incident Management Policy and Procedure and may also be referred to Human Resources and senior management as considered necessary.

5. Policy Review

5.1 This policy will be reviewed by the Data Protection Officer on an annual basis. Formal requests for changes should be sent to the Data Protection Officer Jayne Edwards.

6. Security Policy Framework

6.1 Responsibilities

6.1.1 *Senior Information Risk Owner*

The School's Senior Information Risk Owner (SIRO) or Head teacher has overall responsibility for ensuring there is appropriate technical and organisational security in place to protect the School'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 with [Insert details] and information security rests with [Insert details] who are responsible for implementing, monitoring, documenting and communicating security requirements for the organisation, and keeping the SIRO notified of the effectiveness of the School'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 policies 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 School's Data Protection Policy and the School's mandatory information security guidance, and 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

6.3 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.

6.4 Culture, education and awareness

6.5 An on-going security awareness programme shall be established and maintained to ensure that staff are aware of departmental and corporate security policies 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 Data Protection Officer.

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

6.7 Information security incident management

6.8 Information security incidents shall be reported, recorded and investigated in accordance with the School's Security Incident Management Policy and Procedure. Mitigating actions shall be taken to prevent incidents reoccurring. The Data Protection Officer will be responsible for the management of all information security incidents and will regularly report on trends, risks and mitigations to the SIRO and senior management as required.

6.9 Information risk monitoring and ownership

6.10 The Data Protection Officer will monitor information risks identified during the course of conducting privacy impact assessments, security incident investigations, risk assessments or through direct engagement with services. Information risks are to be recorded on the School's Corporate Information Risk Register.

6.11 The Data Protection 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 Service
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 Service
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.	Senior Information Risk Owner

6.12 Accreditation of ICT systems

6.13 All relevant ICT systems that handle, store and process sensitive information or business critical data, or are interconnected to cross-government networks or services (e.g. the Public Service Network (PSN)), will be risk assessed to identify and understand the relevant technical risks and subject to an annual (or other specified timeframe) PSN accreditation.

6.14 Physical security

6.15 The School 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.

6.16 Personnel security

6.17 The School shall have appropriate personnel security in place to provide assurance as to the trustworthiness, integrity and reliability of its employees. The School will apply Her Majesty's

Government (HMG) recruitment controls described in the Baseline Personnel Security Standard, where required.

6.18 Access control

6.19 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.

6.20 Technical security

6.21 The School 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 School's information.

6.22 Privacy impact assessments and Information Risk Assessments

6.23 Article 29 of the GDPR creates a statutory obligation on Devon County School 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 Officer. All assessments undertaken will be carried out in accordance with the School's Privacy Impact Assessment Procedure.

6.24 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.

6.25 Business continuity and disaster recovery management

6.26 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.

6.27 Freedom of Information Act & Data Protection Act requests

6.28 The School's information and records shall be stored in a manner which facilitates its timely and secure retrieval to enable the School 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.

7.0 Policy History

7.1 This Policy is maintained by the Data Protection Officer and will be reviewed on an annual basis.].