Estyn

Arolygiaeth Ei Mawrhydi dros Addysg a Hyfforddiant yng Nghymru
Her Majesty's Inspectorate for Education and Training in Wales

Information security policy

This document is also available in Welsh.

Information sheet

Information box

For further advice contact: Information Governance Group

Date of publication: July 2021

Version: 1.0

Version control

Document version	Author	Date of issue	Changes made
1.0	Phil Sweeney	July 2021	

Equality Impact Assessment

A business rationale assessment has been carried out and this policy contributes to Estyn’s strategic objectives and delivery principles.

In accordance with Estyn’s Equality Impact Assessment, an initial screening impact assessment has been carried out and this policy is not deemed to adversely impact on the grounds of the nine protected characteristics as laid out by the Equality Act 2010.

Contents Page

1 Introduction

1.1 Background

Estyn is a public body, with information processing as a fundamental part of its purpose. It is important, therefore, that we have a clear and relevant Information Security Policy. This is essential to our compliance with data protection and other legislation and to ensuring that confidentiality is respected.

This document sets out the policy and high level procedures to protect, to a consistently high standard, all our information assets. The policy covers security which can be applied through technology and process controls but perhaps more crucially it encompasses the responsibilities and behaviour of the people who manage information in line with our business.

Information security is about peoples' behaviour in relation to the information they are responsible for, facilitated by the appropriate use of technology. The business benefits of this policy and associated guidance are:

- Assurance that information is being managed securely and in a consistent and corporate way.
- Assurance that we operate a secure and trusted environment for the management of information used in delivering our business.
- Clarity over the personal responsibilities around information security expected of staff when working for us.
- A strengthened position in the event of any legal action that may be taken against us (assuming the proper application of the policy and compliance with it).
- Demonstration of best practice in information security.
- Assurance that information is accessible only to those authorised to have access.
- Assurance that risks are identified and appropriate controls are implemented and documented.

1.2 Aim

The aim of this policy is 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.

1.3 Objectives

The objectives of this policy are to establish and maintain the security and confidentiality of our information, information systems, applications and networks by:

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

1.4 Scope

Staff working in or on our behalf (this includes contractors, temporary staff, staff seconded/loaned and all permanent employees) are within the scope of this policy.

2 Roles and responsibilities

2.1 Her Majesty's Chief Inspector (HMCI)

Responsibility for information security resides ultimately with HMCI. This responsibility is discharged through the designated roles of Senior Information Risk Owner (SIRO).

2.2 Senior Information Risk Owner

The Senior Information Risk Owner (SIRO) is responsible for information risk within Estyn and advises the Executive Board and Strategy Board on the effectiveness of our information risk management. This role is currently designated to the Director of Corporate Services (Phil Sweeney).

2.3 Data Protection Officer (DPO)

As a public authority we are required to appoint a Data Protection Officer by the General Data Protection Regulation (GDPR). The DPO is responsible for providing advice, monitoring compliance, and is the first point of contact in the organisation for data protection matters. The DPO reports to the SIRO and directly to the Executive Board and Strategy Board in relation to data protection matters.

2.4 Information Asset Owners (IAOs)

IAOs are responsible for the security of their environments (physical and digital) where information is processed or stored. Furthermore, they are responsible, in conjunction with managers, for:

- Ensuring that all staff, permanent, temporary and contractor, are aware of the information security policies, procedures and user obligations applicable to their area of work to maintain good information security
- Determining the level of access to be granted to specific individuals
- Ensuring staff have appropriate training for the systems they are using
- Ensuring staff know how to access advice on information security matters

All IAOs are responsible for ensuring that third party data processors have appropriate ISO and/ or Cyber Essentials accreditation where appropriate for assets stored electronically with third parties. IAOs are also responsible for ensuring appropriate data protection assurance from all third party suppliers processing our data.

2.5 Chair of Information Governance Group (IGG)

The Chair of IGG will be responsible for maintaining appropriate policies and guidance for staff around the use and processing of personal data of information contained within our information assets in line with data protection and data security legislation and regulations.

2.6 IT Cyber Security Officer

The role of the Chair of IGG is supported by the IT Cyber Security Officer (ITCSO).

The ITCSO is responsible for developing, implementing and enforcing suitable and relevant information security procedures and protocols to ensure our systems, equipment and infrastructure have adequate security measures to comply with data protection and data security legislation and regulations.

2.7 All staff

All staff are responsible for information security of the data that they use or have access to through their employment with Estyn and therefore must understand and comply with this policy and associated guidance. Failure to do so may result in disciplinary action. In particular all staff should undertake their mandatory annual Information Security Awareness training and understand:

- What information they are using, how it should be protectively handled, stored and transferred
- What procedures, standards and protocols exist for the sharing of information with others
- How to report a suspected beach of information security within Estyn
- Their responsibility for raising any information security concerns with the ITCSO and SIRO

3 Policy framework

3.1 Contracts of employment

Staff security requirements shall be addressed at the recruitment stage and all contracts of employment shall contain an appropriate confidentiality clause.

Information security expectations of staff shall be covered within the induction process and referenced within appropriate job definitions and descriptions.

3.2 Security control of assets

The Office Services team will establish and maintain an IT asset management process and associated system; all IT assets, (hardware, software, application or data) shall have a named Information Asset Owner (IAO) who shall be responsible for the information security of that asset.

In order to minimise loss of, or damage to, all assets, the Office Services team shall ensure that all electronic equipment and assets shall be; identified, registered and physically protected from threats and environmental hazards.

3.3 Access controls

Access to information shall be restricted to users who have an authorised business need to access the information and be in line with approval by the relevant IAO.

System owners must ensure that access controls are maintained at appropriate levels and that any changes of access permissions are authorised. A record of access permissions granted must be maintained. Access to all IT Systems must use a secure login process and access may also be limited by time of day or by the location of the initiating terminal, or both.

Line managers must ensure that access to IT systems is only available to employees during their period of employment. In particular, line managers must ensure that the system access of leavers is withdrawn as soon as employment is terminated; the HR team will maintain a checklist of system access removals.

Access to data, system utilities and program source libraries shall be controlled and restricted to those authorised users who have a legitimate business need e.g. systems or database administrators. Authorisation to use an application shall depend on the availability of a license from the supplier.

Contracts with external contractors that allow access to our information systems must be in operation before access is allowed. These contracts must ensure that the staff or sub-contractors of the external organisation comply with all appropriate security policies.

3.4 Computer and network procedures

Management of computers and networks shall be controlled through standard documented procedures. This will also require agreed systems and processes with outsourced IT support and third party vendors working for and on behalf of Estyn.

3.5 Information risk assessment

All information assets will be identified and assigned an Information Asset Owner (IAO). IAO's shall ensure that information risk assessments are performed at least annually, following guidance from the Senior Information Risk Owner (SIRO). IAO's shall submit the risk assessment results and associated mitigation plans to the SIRO for review at meetings of the IGG. The IGG will maintain and review an overarching Information Risk Register.

3.6 Information security events and weaknesses

All information security events, near misses, and suspected weaknesses are to be reported to the SIRO and ITCSO. The Information Security Incident Reporting procedures must be complied with.

3.7 Classification of sensitive information

We will implement appropriate information classifications controls, based on the results of formal risk assessment and guidance contained within the Information Assurance Policy and relevant desk instructions.

3.8 Protection from malicious software

We will work with IT service providers to use software countermeasures and management procedures to protect against the threat of malicious software. All staff shall be expected to co-operate fully with the IT Usage Policy, e.g. individuals shall not install software without the appropriate permission.

3.9 Monitoring system access and use

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis to support compliance checks with this and other policies, and, if necessary, monitor activity where there is a suspected breach of policy. The Regulation of Investigatory Powers Act (2000) permits monitoring and recording of employees' electronic communications (including telephone communications) for the following reasons:

- Establishing the existence of facts
- Investigating or detecting unauthorised use of the system
- Preventing or detecting crime
- Ascertaining or demonstrating standards which are achieved or ought to be achieved by persons using the system (quality control and training)
- In the interests of national security

- Ascertaining compliance with regulatory or self-regulatory practices or procedures
- Ensuring the effective operation of the system.

Any monitoring will be undertaken in accordance with the above act and the Human Rights Act and any other applicable law.

3.10 System change control

Changes to information systems, applications or networks shall be reviewed and approved by the ITCSO in conjunction with the System Owner. System Owners must ensure that the procurement or implementation of new or upgraded software is carefully planned and managed and that any development for or by Estyn always follows a formalised development process with appropriate audit trails. Information security risks associated with such projects must be mitigated using a combination of procedural and technical controls. Business requirements for new software or enhancement of existing software must specify the requirements for information security controls.

3.11 Accreditation of information systems

We shall ensure that all new information systems, applications and networks include a System Level Security Policy (SLSP) and are approved by the ITCSO before they commence operation. All systems will have a designated System Owner. The SIRO must approve:

- Any new process that involves processing of personal data (data relating to individuals)
- Changes to be made to an existing process that involves the processing of personal data
- Procuring a new information system which processes personal data, or the licensing of a third-party system that hosts and or processes personal data
- Any new technology that uses or processes personal data in any way

3.12 Business continuity and disaster recovery plans

Business continuity plans will be put into place by Systems Owners to ensure the continuity of prioritised activities in the event of a significant or major incident.

The SIRO will seek assurances from System Owners that appropriate disaster recovery plans are in place for all priority applications, systems and networks and that these plans are reviewed and tested on a regular basis to provide evidence that backup restoration and recovery processes are effective.

3.13 Training and awareness

Information security training is mandatory and all staff are required to complete on-line training in line with scheduled periods. All staff are required to confirm that they have read relevant policies designated within our information governance framework – regular updates related to information governance and security matters will be provided, along with checks on awareness around issues and risks such as phishing attempts and ransomeware risks.

4 Monitoring

Compliance with the policies and procedures laid down in this document will be monitored via the IGG, together with independent audit reviews on a periodic basis. The IGG will also be responsible for updating this document and related policies and guidance, and for identifying ongoing and emerging staff training needs.