Estyn

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

Information Assurance Policy

This policy is also available in Welsh.

Information sheet

Information box

For further advice contact: Information Governance Group

Date of publication: July 2021

Version: 4.0

Version control

Document version	Author	Date of issue	Key changes made
1.0	Phil Sweeney	May 2012	
2.0	Information Governance Group	December 2013	Updated to reflect changes to Gov't Protective Marking Scheme
2.1	Information Governance Group	March 2016	Minor amendments following internal audit
3.0	Information Governance Group	May 2018	Updated to reflect introduction of the General Data Protection Regulations
4.0	Information Governance Group	July 2021	Tone of voice. Added guide on 'handling instructions'. Removed appendices ('Protective markings' and 'Arrangements for sending information by email and by post') – these are covered by local desk instructions issued by relevant IAO.

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

Section 1: Introduction

1 Estyn has a duty to maintain the security of information it handles - this means protecting data from unauthorised access, ensuring its accuracy and integrity, and maintaining availability of the information to those who need it.

2 This policy is part of our framework of policies and procedures on information governance, and it applies to all employees and people working on our behalf. Staff and other people working for us must follow the rules, policies and guidelines we have developed. They must also understand their personal responsibilities when creating, sharing and storing information in relation to our work.

3 Line managers are responsible for making sure that agency staff comply with this policy. For external inspectors and other individuals who work for us (e.g. through contracts for services and memoranda of understanding), compliance with this policy will be included in the agreements, terms and conditions and guidance we issue when they start working for us.

Our approach to information governance

4 The following points describe our approach to information assurance:

- The Information Governance Group has responsibility for overseeing our information-related policies and risk management. The group is also responsible for providing guidance and training to staff on how to handle information.
- A named person (Information Asset Owner or ‘IAO’) will be responsible for the information held in each system or work area. They will receive additional training.
- IAOs will be responsible for identifying all types of information (information asset) held, generated or received by their business area, and for making sure it is stored in appropriate systems.
- Information assets will be classified with a protective marking, according to their sensitivity and how serious disclosure or loss of the information would be. These protective markings are defined by government guidelines. IAOs are responsible for communicating and monitoring the use of these markings and handling instructions within their business area.
- The IAO will be responsible for assessing the risks associated with holding each information asset, and for identifying ways to remove, mitigate or accept these risks.
- The IAO may escalate the ownership and management of the risk to an appropriate level in line with our Risk Management Policy.
- We will maintain and follow a process for reporting on and managing information-related incidents.

5 The overall rules for information handling are determined by IAOs and other senior staff. For individual pieces of information, the responsibility to keep the information safe is with the direct receivers, users and holders of that information. The day-to-day use and handling of information will be managed by all staff, who we will support with training and guidance.

Section 2: Classification of information - protective markings and secure handling

Protective markings

6 The Cabinet Office has mandated the use of protective markings to help protect government information – we will use these markings to indicate the sensitivity of an 'asset'.

7 Individual documents and data relating to the information asset should be physically (electronically) marked when they are created. However, in some areas (for example on emails or paper documents) the originator or receiver of the document must ensure the protective marking is applied. By default, we will maintain the classification level specified by the source. If the source doesn't provide a classification, or if an unrecognised classification has been used, the recipient must review the content and protectively mark the information as appropriate.

8 Our information must be labelled with the appropriate protective marking. These markings must be in bolded capital letters, and in the headers and/or footers of the document.

9 The majority of our information is expected to be unclassified and require no protective marking. The only level of classification used within Estyn will be **OFFICIAL.**

10 If information marked as **OFFICIAL** is compromised, it is likely to:

- cause significant distress to individuals
- be a breach of confidence, reducing people's trust in us
- breach statutory restrictions on the disclosure of information

11 Depending on the severity of the circumstances it could:

- cause financial loss, or facilitate improper gain or advantage for individuals or companies
- prejudice the investigation or facilitate the commission of crime
- disadvantage government in commercial or policy negotiations with others
- impede the effective development or operation of government policies
- breach statutory restrictions on the disclosure of information
- undermine the proper management of the public sector and its operations

12 The **OFFICIAL** marking should be followed by a handling instruction. Examples include:

- '*For the addressee only'* – only the person the information was originally sent to should see it
- '*For HR use only'* – the information should not be shared outside of HR (similar instructions can be used for other groups, e.g. SMT)
- '*Consult the originator before sharing further'* – ask the person who created the information if you can share it with someone else you think needs to see it

- '*Do not share externally'* – this might apply to information that is for internal use only or a document that is not ready for publication, e.g. a draft inspection report or a publication under embargo

13 IAOs should include the handling instructions for information and documents requiring protective marking that are recorded in their Information Asset Registers. Protective marking and handling instructions should be included, as appropriate, on template forms and other documents and be referenced within relevant desk instructions for the processing of information. A blank form will only require a marking if it contains sensitive information. Some blank forms which always contain sensitive information on completion may be printed with the marking already applied. The Information Governance Group will review these registers annually to make sure they are appropriate.

14 When information is updated, you must reconsider the impact level and associated handling process. The impact level may change over time, for example when a document is published.

15 If information is aggregated together in a single place (for example a database, filing cabinet, or encrypted external storage device) the impact level must be considered for the combination of the information. It must also be marked clearly on the cover. The marking must reflect the highest level of sensitivity of any individual item within the collection of data.

Access to protectively marked information

16 We operate an open policy for sharing unclassified information. However, access to protectively marked information may need to be internally restricted.

17 IAOs are responsible for overseeing the access provided to information; access should be provided on a need-to-know basis, particularly where the data is sensitive.

18 IAOS and managers must provide guidance on data handling to anyone with access to sensitive data stored on our systems. This guidance will usually be through desk instructions for the particular business process. Individuals are responsible for following these instructions.

19 IAOs should regularly review access rights to protected systems and information to make sure that that staff members who change roles or leave the organisation have their access rights amended or removed.

20 When new business processes are established that will require the use of protective markings, the IAO must carry out a risk-assessment before the process is implemented. This includes setting up access rights.

21 In some circumstances protectively marked information may have to be disclosed to the public under Freedom of Information requirements.

Protecting sensitive information

22 Staff must make sure that protectively marked information is not disclosed to another person unless that person is authorised to receive it.

23 When you are reading and reviewing information, you should be aware of the risk of data loss. Do not leave documents marked as **OFFICIAL** unattended, for example on desks or printers in the office or home. Please follow our clear desk policy by locking away protectively marked documents when you leave your desk unattended, e.g. when you go for lunch or finish work at the end of the day.

24 Do not discuss any sensitive information in a public place where you could be overheard. Even in work situations, consider who may be able to hear your conversations, telephone calls or video conferences, and move to a private room if needed.

25 The Chair of meetings is responsible for ensuring that those in attendance are entitled to access the information being discussed. If you are attending a meeting and you are unsure of what you can say (or hear), then ask the Chair to confirm.

26 You should always lock your computer when you move away from it by holding down CTRL+ALT+DEL then pressing Enter. Turn your computer off completely when you have finished work for the day, or if you will be away from it for a long period of time.

27 Storage of information on removable media can present a greater risk of loss or inappropriate sharing - follow the IT Usage Policy when using removable media.

28 Never save sensitive data to the hard drive of desktop computers. Unlike laptops, our desktop computers are not encrypted and they do not provide the right level of data protection if the device is stolen or accessed by someone other than the user. Use your Y Drive or One Drive to save any data locally.

29 You should take all reasonable measures to protect your laptop in line with our IT Usage Policy, whether they are in transit or in your home. Remember that laptop encryption only works when the computer is fully turned off.

30 You can minimise the risk of data being read by unauthorised people by:

- reducing the amount of paper information you keep with you or store at home
- only printing documents when you absolutely need to
- storing protectively marked documents securely (e.g. in a filing cabinet) when they're not in use

31 You should delete emails and files as soon as they are no longer required.

32 You must dispose of information in a way that makes recovery or retrieval of the content unlikely. The IT Security Officer (ITCSO) is responsible for overseeing the secure disposal of all IT equipment.

33 In the office, you should use the appropriate paper disposal bins to dispose of sensitive information. At home, store any sensitive documents securely and dispose of them in the main office, if possible, or use a shredder.

Third parties

34 Staff who are responsible for engaging third parties should make sure that suppliers abide by this policy. All formal terms and conditions for suppliers include protocols for data protection which must be followed.

Section 3: Reporting information security incidents and near misses

35 An information security incident happens when sensitive information is lost, stolen, or is released to or accessed by unauthorised parties, for example:

- loss of a laptop or removable media
- attempted or actual unauthorised access to sensitive data in one of our systems
- unauthorised disclosure of information about staff or those we inspect
- sending an email or letter to one or more incorrect addresses
- reported non-receipt of email and postal mail

36 All staff have a responsibility to report a security incident as soon as they become aware of any possible loss of data. Responding quickly is critical to increasing the chance of recovering the data and reducing the impact of a data loss. Failure to report or an unnecessary delay in reporting an incident may have serious consequences. Under the General Data Protection Regulations, certain personal data breaches must be reported to the Information Commissioner's Office within 72 hours.

37 Staff must report any incident to both the IT Cyber Security Officer (ITCSO) and their line manager as soon as possible.

38 Failure or refusal to report a known incident may result in disciplinary action. Failure or refusal to report a known incident by any non-staff member undertaking work for Estyn may result in termination of their contract or agreement.

39 A **near miss** is defined as any incident which exposes or potentially exposes information to unauthorised access or loss. This could include occasions where our practice or actions deviate from our security policies or procedures.

40 Individuals also have a responsibility to report **potential** security incidents to the ITCSO and their line manager, or by using the Whistleblowing Policy and Procedure if they want to remain anonymous.

41 The ITCSO, along with our Data Protection Officer (DPO), is responsible for incident management. They will involve other individuals such as an IAO in this process when it is appropriate. The ITCSO will record details of the incident in a log and will help to draft an action plan to contain the incident, notify those affected and prevent a similar incident happening in future.

42 The ITCSO is also responsible for maintaining logs and informing the relevant Government organisations of any incidents which are considered 'Notifiable' by the

relevant agencies, or which are required by legislation. The ITCSO will report any incidents to the Information Governance Group to help with future risk management and to identify any requirements for further staff training or documentation.

Section 4: Project management and information assurance

43 This section provides guidance for managers of projects or programmes. Projects, for example thematic reports, can involve changes to the way we collect or use information, and information assurance should be built into the project at the outset.

Data protection impact assessment

44 At the start of a project, the project manager should decide whether a Data Protection Impact Assessment (DPIA) is needed.

45 DPIAs are a risk management technique and should be started early in the project management process to identify risks and make sure the project is designed appropriately. You can get further guidance and templates from The Information Commissioner's Office (ICO) and from the Information Governance Group.

46 Where there is a procurement element to a project or programme, contracts should include clauses to ensure that contractors understand and adhere to Government standards for secure information access and management. Please contact the Procurement Compliance Officer for more advice.

47 The project board for each project is responsible for ensuring compliance with the approach to information assurance outlined in this section. The project board should make sure that any data or information transfers outside our organisation are authorised by the IAO.

Section 5: Internal and external communications

48 You must take care when you exchange information with other organisations, particularly sensitive information. This includes exchanges of information with both government and private sector organisations. You should only exchange information with recognised partners as part of agreed business processes.

49 All business processes which could include regular or occasional exchanges of sensitive information must be documented and risk assessed by the IAO. This is to make sure that security requirements are understood by everyone involved and that the transfer is managed in an auditable way. Regular personal data sharing with an external organisation should be logged on the Information Asset Register.

50 When you transfer information or documents, you should remove any unnecessary data fields that are not needed to carry out the business function. This could include deleting columns we use internally but which the other party doesn't need to carry out their work.

Emails must be marked according to the sensitivity of the information they contain, including any attachments. If the information is protectively marked, the email must be labelled with the appropriate protective marking and handling instruction **at the beginning** of the subject line. The identity of online recipients, such as email addresses, should always be checked carefully prior to dispatch.

51 Personal data that if lost or inappropriately shared could be subject to reporting to the Information Commissioner's Office as a personal data breach (broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data) must be given extra protection, e.g. encrypted or password protected before it can be emailed to someone outside the organisation. Please contact the ITCSO and the IGG for advice on how to do this.

52 If you identify a new requirement for exchanging electronic data with a third party, you should raise this with the IGG to identify the most appropriate method of transfer.

53 Do not send protectively marked documents to a personal email account (e.g. Hotmail, Google or Yahoo). You can find further rules and guidance on using email in the IT Usage Policy.

54 If you are sending data to or receiving data from any other organisation, you must agree the level of sensitivity and appropriate handling procedures with the source of the data. Where data is shared regularly, the handing arrangements should be more formally agreed, for example as part of a Data Access Agreement, Memorandum of Understanding or Service Level Agreement.

55 The Cabinet Office has strict rules about sending sensitive information abroad. Please contact the ITCSO for advice if you have any sensitive information which needs to be sent abroad.

56 If you are unsure about anything in this policy please contact a member of the IGG for advice.