Pecyn Cymorth Llywodraethu Gwybodaeth Cymru
Welsh Information Governance Toolkit
IGDC • DHCW

Expectations Guidance Document

1.2 – Policies and Procedures

Introduction

This guidance will provide basic information on what will be required from Organisation Administrators and Users to work through and complete the 'Policies and Procedures' section of the Welsh Information Governance Toolkit (WIGTK).

It is the responsibility of the organisation to implement appropriate technical and organisational measures to ensure information is processed lawfully. The implementation of policies and procedures is a key element of these measures.

Your policies and procedures should outline how the organisation will meet its information governance responsibilities and will provide staff with the direction to understand their roles and responsibilities.

In addition, operational procedures and guidance should be implemented to support the above policies and provide direction to staff.

You will need to consider policies which are held across your whole organisation for this section.

Please note, in this section of the WIGTK you will be required to upload copies of the relevant policies if you have ticked that your organisation has them available.

Minimum Expectations

Policy Setting and Availability
As a minimum, the organisation should have policies in place that cover a range of information governance matters including:

- Data Protection/Information Governance,
- Records Management,
- Information Security, and
- Data Quality.

Within your policies, the following should be clearly stated:

- the responsibilities that all staff have regarding information governance
- how the organisation only collects, uses and shares the minimum amount of data necessary for the purpose
- how the organisation ensures that data is only available to those who need it
- how the organisation stores data only for as long as is needed
- how the organisation informs individuals what is being done with their data

Your policies and procedures should outline how the organisation will meet its information governance responsibilities and will provide staff with the direction and clarity to understand their roles and responsibilities regarding information governance.

In addition, operational procedures and guidance should be implemented to support the above policies and provide direction to operational staff.

The organisation's policies and procedures should outline the responsibilities of all staff, as well as the responsibilities of staff who play key roles in information governance or relevant processes, such as the IG Lead, Caldicott Guardian and DPO to provide consistency.

Staff should be fully aware of the information governance policies and procedures that are relevant to their role.

Policies, procedures, and guidance materials should be made available to staff in an easily accessible format. For example, organisations who have an internal intranet site, this may include publishing policies here. Alternatively, shared areas may be used, such as shared drives or physical copies of guidelines and key messages distributed.

Further information on the requirements and support are set out within the Policies and Procedures expectations of the ICO's Accountability Framework.

Monitoring Compliance with Policies

Conducting audits of policies and procedures can allow your organisation to determine if policies and procedures are being implemented and followed correctly, allowing you to review their effectiveness. For example, by conducting spot checks, ensuring staff are aware of the policy, can locate it, are aware of their role and that the requirements outlined are followed and work in practice.

Data Breaches

Your organisation should have policies or procedures in place relating to dealing with personal data breaches and how they are detected, recorded, and managed.

Staff within your organisation must be able to detect, investigate, risk-assess, and record any breaches effectively. The organisation must report data breaches as appropriate. Having effective policies and processes in place will help to achieve this.

Policies and procedures should clearly outline a consistent method for the assessment of breaches, as well as the threshold for notification to the ICO and data subject. The process for notifying the ICO of a breach within 72 hours of becoming aware of it should be outlined, along with details of what information must be given to the ICO about the breach.

Your policy or procedure should also outline how you review and monitor breaches within the organisation and track any trends and patterns and identified ways to mitigate these to prevent incidents reoccurring.

The requirements for detect, manage and record are set out within the Breach Response and Monitoring expectations of the ICO's Accountability Framework.

Access Requirements
Article 5(1)(f) of the UK GDPR states:

"1. Personal data shall be:
(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction, or damage, using appropriate technical or organisational measures ('integrity and confidentiality')."

Your organisation must limit access to personal data, to authorised staff only and regularly review users' access rights to make sure it is kept accurate and up to date.

The organisation should have an agreed upon process for the granting, restriction, review, and removal of staff access to the premises and any systems which contain personal data.

This process may be recorded within the organisation's Information Security Policy, System Acceptable Use Policies or a Starters, Leavers, and Mover's procedure.

FOI & EIR – Not applicable to Third Party Contractors
Your organisation should have an established process for the management of its FOI & EIR responsibilities. This should be recorded within a procedure or other relevant guidance and include the high-level responsibilities of staff.

The procedure should include the recognition of FOI & EIR requests received into the organisation, the processing of these requests, and the organisation's publication scheme commitments.

Disposing of Confidential Records
In line with Article 5 1(e) of UK GDPR, it is important that when personal data is no longer needed for the purpose for which it was collected that it is disposed of securely. This applies to paper documents, electronic records, and equipment, such as old computers and laptops, mobile phones, CDs, and memory sticks.

If anyone in your organisation destroys any records or equipment themselves, such as shredding documents, the organisation should have policies, procedures, or guidance documents available for staff to ensure they understand how to destroy the data securely.

Exceeded Expectations

This section is not required to be completed; however, it will help to further demonstrate your compliance and provide assurance.

These questions build on those you will have answered in the minimum expectations section; however, they are slightly more in depth.

Approval Process

The ICO expects there to be a review and approval process in place to make sure that policies and procedures are consistent and effective across the organisation.

An appropriately senior staff member, such as Board or Committee, should review and approve all existing, new, and updated policies and procedures. The individual/group who is responsible for approving the document should be detailed within the policy and procedure.

Policies and procedures should be reviewed and updated without undue delay when they require changes and should show document control information, including version number, owner, review date and any change history.

The requirements review and approval are set out within the Policies and Procedures section of the ICO's Accountability Framework.

Actively Informing Staff

The organisation should have an effective process to communicate updates on new and reviewed policies and procedures to ensure staff are fully aware of the relevance to their role. This may be done through all staff round robin emails, inclusion in staff newsletters, bulletins, or news item updates on the organisation's intranet site.

Record of Understanding

It is best practice to keep a record of staff's understanding of the various policies and procedures in place.

For policies and procedures to be effective, staff must read and understand them, and know why they are important to implement and comply with.

The organisation should keep a record of confirmation that staff have read and understood relevant policies and procedures to their role, including:

- Information Governance/Data Protection
- Records Management
- Information Security
- FOI & EIR
- Data Incidents

This may be done by holding a central electronic register of staff confirmation statements, or by implementing a process whereby line managers retain declarations of understandings within staff files.