Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Internal

Information Security Policy & Guidance

Policy Statement

Information held by the Office of the Future Generation Commissioner is a significant asset. In carrying out our roles we may access, create and use a wide range of information; we rely on the integrity, availability and confidentiality of information to support our work and fulfil the Commissioner's statutory functions.

This policy outlines our approach to information security management and provides the guiding principles to support and safeguard our information systems; these principles apply to all our information assets in electronic and physical formats.

The General Data Protection Regulation (GDPR), Freedom of Information Act (FOIA) and Environmental Information Regulations (EIRs) place duties and responsibilities on the Commissioner in respect of the information we hold.

The Commissioner expects that all staff and associates familiarise themselves with the Information Security Principles contained in this policy and to apply appropriate controls to manage our information security risks.

Information Security Principles

While all staff are required to adhere to the requirements of this policy, staff with particular responsibility for information management are:

Commissioner

Director of Finance and Corporate Governance

Director of Policy, Legislation and Innovation

Director of Communications, Engagement and Partnerships

Data Protection Officer (DPO)

Access Controls

- Our information management systems have been set up to ensure that all staff have access to the information resources appropriate to their role.
- Access controls are in place to ensure that personal information is only accessible to certain categories of staff for limited purposes.

- These access arrangements are reviewed regularly.
- If you believe your access arrangement is incorrect you should raise this with the DPO immediately.

Email: sharing information, restricting access

- As the email creator it is your responsibility for instructing recipients what can be done with the data contained in the message. E.g. Do not circulate - check with me as information originator.
- As the recipient it is your responsibility to ensure you do not share information inappropriately particularly with others **outside** the organisation. If in any doubt – check before sharing.

Review of Arrangements

- We carry out an annual review of information security arrangements including assessment of current cyber security risks and a review of incidents and near misses. This review will inform future plans and any necessary changes to our security arrangements.
- If circumstances or risks change and immediate actions and changes are needed all staff will be informed and this policy updated.

Implementation of New Systems

- All new ICT systems e.g. phone services, databases, CRM system - are subject to the requirements of this policy and staff responsible for the development and implementation of these systems are expected to ensure information security issues are addressed at the earliest stage.

Suppliers

- All our suppliers will be required to demonstrate they are able to adhere to the principles of this policy.
- Our IT Support Services are currently provided by Orbits IT. This arrangement is due for review in 2018.
- Services and standards underpinning this contract are set out in a Service Level Agreement (SLA) and a data processor/sharing contract.

Cloud Providers

- The GDPR requires that we have appropriate technological measure in place to ensure our data is secure. Even where our data is stored through cloud based services we retain responsibility as the data controller and will therefore be responsible should a breach occur.

- Our cloud service providers will therefore be expected to demonstrate it meets GDPR standards of **privacy by design** and that it has considered information security as a fundamental principle in its service delivery.

Any breach of personal data

- Our IT Support Services are currently provided by Orbits IT. This arrangement is due for review in 2018.

- Services and standards underpinning this contract are set out in a Service Level Agreement (SLA)

Compliance & Awareness

- Training
    - all staff will be provided with appropriate awareness guidance and training
    - Training will be provided for new starters as part of their induction
- Advice
    - You can seek advice about this policy and its requirements from any member of the senior team or your designated DPO

Monitoring and Disciplinary Action

- Access and use of our systems is regularly monitored to ensure the security and integrity of the data we hold and any inappropriate activity will be investigated and could be subject to disciplinary action.

- All staff should familiarise themselves with our IT Acceptable Use Policy.

- Any security breach could lead to data loss, breach of confidentiality and availability of information held on our systems. Data loss or loss of access to information held by the Commissioner means we cannot comply with our duties under FOIA and EIR.

- Any breach of confidentiality of personal data would be a contravention of the GDPR and could result in fines or other action against the Commissioner.

Incident Reporting and Management

- Any security breach will be managed as set out in our Data Breach Policy & Guidance.
- All staff and associates are expected to report any loss or breach and any issues of concern. Early intervention is key as it may help us to minimise the impact of a breach or reduce the risk of escalation.
- You can make a report or raise an issue with any member of the senior team or with the DPO.

Related Policies

Information Governance Policy

IT Security & Acceptable Use Policy

Freedom of Information (FOI) & Environmental Regulations Policy

Data Protection Policy

Access to Information Guidance

Data Breach Policy

Internal

Guidance - Keeping Information Safe

Do

- Do ensure your mobile devices are encrypted/complex password protected
- Do ensure you comply with requests to change passwords
- Do ensure you comply with requests to update your systems
- Do ensure you understand and apply any agreed document/email marking systems
- Do ensure you are aware of arrangements for protecting personal information
- Do ensure you are aware of arrangements for sharing personal data
- Do ensure you understand what 'special categories' of personal data are and the actions you should take.
- Do report any concerns before reconnecting a laptop or other device to the network.

Don't

- Don't reveal IT passwords to anyone
- Don't leave your PC or laptop unlocks
- Don't store a written password with your laptop or mobile device
- Don't reveal IT security arrangements to 3rd parties/supplies without written contractual agreement
- Don't forget the physical environment – office space, written notebooks, post-its, flip charts.
- Don't leave visitors to the office unattended.
- Don't attempt to introduce any new software or files to the Commissioner's system without written permission of the Office Manager.

- Don’t use any personal portable media or external drives; they could compromise the integrity of the Commissioner’s IT systems.

- Don’t forward emails containing personal data without checking with the email originator