Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Internal

Personal Data Breach Policy

Policy Statement

The Commissioner is committed to ensuring that all personal and corporate information is held appropriately in accordance with the requirements of the Data Protection Act (DPA), General Data Protection Regulation (GDPR), Freedom of Information Act (FOIA) and Environmental Information Regulations.

The Commissioner expects that all staff and associates comply with the requirements of this policy and to raise any concerns or issues promptly so that risks to the personal data we hold may be minimised.

Roles and Responsibilities

- Director of Director of Finance and Corporate Governance
- Head of Human Resources
- Data Protection Officer (DPO)
- Finance and Corporate Governance Officer
- Office Manager

Personal Data Breach Policy

The General Data Protection Regulation (GDPR) requires that we have this policy in place.

What is a Personal Data Breach?

A personal data breach can be broadly defined as a security incident that affects the confidentiality, integrity or availability of personal data.
GDPR broadens the definition of a data breach to include:

- Access by an unauthorised third party
- Deliberate or accidental action (or inaction) by a controller* or processor
- Sending personal data to an incorrect recipient
- Devises containing personal data being lost or stolen
- Alteration of personal data without permission
- Loss of availability of personal data

A data breach or loss may also impact on our ability to fulfil our responsibilities under FOIA as information subject to FOI may not be available.

*Joint data controllers have joint liabilities in the event of a breach.

Duty to Notify Information Commissioner's Office (ICO)

In certain circumstances we are required to report a breach/loss Information Commissioners Office within 72 hours and to inform the data subject without undue delay (should the breach potentially impact on the rights and freedoms of the data subject). This must be assessed on a case by case basis and any decision **not to notify** must be recorded.

Reporting and Scrutiny – All staff and associates are expected to flag any concerns or issues with the DPO or Office Manager immediately; we may be able to prevent or minimise risk of breach or loss.

Actual or near miss data/loss incidents will be regularly reported through the Commissioners senior staff team to the Commissioner and her Audit Committee.

Penalties and Fines – GDPR allows the ICO to apply significant monetary penalties in relation to data breach or loss. This includes failure to have policy in place, failure to inform ICO or data subject of breach (if appropriate).

Technical and Organisational Measures

We are required by the GDPR to apply appropriate technological and organisational measures to ensure personal data is held securely and processed in accordance with the rights of data subjects. We work with an external IT supplier (currently Orbits IT) who provide hardware, network and cloud based services to support our working practices.

The following measures are in place to ensure that our data is protected from external threat:

1. All devices under Orbits IT management require unique, strong passwords which are changed on a regular basis
2. Systems are updated and patched to a regular schedule when updates available from manufacturer
3. Internal networks protected by both hardware and software firewalls with regular vulnerability scans carried out and actioned upon.

4. Client devices managed by Orbits are protected by antivirus and security software (Webroot).
5. Standard users have no administrator access to devices
6. Web traffic is routed through secure DNS systems to filter by content and category as well as providing cybersecurity.
7. Cloud services are provided by Microsoft 365

Orbits IT act as our data processor and our IT support services are defined in a formal contract and service level agreement (SLA). The contract and SLA includes descriptions of how Orbits IT ensure that a) our data is protected from external threat and b) arrangements for data recovery should a breach or loss occur.

As our data processor, Orbits IT has a duty to inform us of any incident that affects personal data. Should an incident occur that affects personal data Orbits IT will report this to one of the primary contacts by email with a follow up telephone call – The primary contacts are currently Sang-Jin Park, Susan Crutcher or Helen Verity.

The response to a breach depends on the nature of the incident. Orbits IT will work with FGC staff to determine best approach to containment and to minimise risk of further data breach or loss. These could include the restoration of data from backups, remotely wiping devices of data and analysing the audit trail for the data in question.

How can a breach or loss occur?

A data breach or loss can occur in a number of ways.

Systems

Technical external breach that affects part or whole of network

Technical failure e.g. loss of network, back up failure

People

Accidental e.g. clicking an unknown link, using an unknown data stick, downloading an unchecked document, loss of data stick, mobile, laptop or tablet.

Malicious action - e.g. purposefully downloading malware, theft, sabotage

Our Approach

Our information governance policies and procedures are designed to minimise the likelihood of a breach or loss occurring, however it is important that all staff and associates continue to be aware of the risks.

A data breach or loss can have significant impacts to data subjects (including each of us). As a public body we could be subject to fines and a significant loss of public confidence.

- We have reviewed all our information governance arrangements and updated our policies and procedures
- We have appointed a Data Protection Officer (DPO) to provide information and guidance.
- We have provided information and training sessions for staff and associates
- We have developed guidance to support staff responding to a data breach/ loss (Appendix A).

Related Policies and Documents

Information Governance Policy

IT Security & Acceptable Use Policy

Information Security Policy

Freedom of Information (FOI) & Environmental Regulations Policy

Data Protection Policy

Access to Information Guidance

Data Sharing Contract and Service Level Agreement (SLA) with Orbits IT;

Sources of Advice and Guidance

Data Protection Officer (DPO) Sang-Jin Park

Information Commissioner's Office – Wales
2nd Floor, Churchill House
Churchill Way, Cardiff, CF10 2HH
Telephone: 029 2067 8400
Fax: 029 2067 8399
Email: wales@ico.org.uk

Further information can be found at www.ico.org.uk

Appendix A: Responding to a Data Breach/Loss: Actions to take

A possible breach* has occurred: 1. Take any action that will prevent further breach or loss or that will minimise impact of breach 2. Inform senior staff of breach/loss 3. Check immediately with staff to ensure no unauthorised action that could impact on the breach/loss is taken	Note date and time of breach Note any actions taken *Joint data controllers have joint liabilities in the event of a breach*
Working with Orbits IT evaluate: 1. How breach/loss occurred and any actions to take to reduce impact or mitigate risks 2. The scale of data breach/loss (type of information affected, volume of data) 3. Potential of further breach or loss 4. Likely impacts on data subject(s) From this identify any further actions required.	Keep detailed contemporaneous notes (to assist in completing report to ICO or audit committee) Further actions will likely depend on type of breach and scale of any loss NB malicious actions or failure to adhere to policy/ procedures could lead to disciplinary action. Check with HR re actions to take.

If applicable - within 72 hours – inform ICO of breach providing the following information: 1. Date and time of incident 2. How breach/loss occurred 3. The scale of data breach/loss 4. Potential of further breach or loss 5. Likely impacts on data subject(s) 6. Actions taken to date to minimise further loss or to mitigate affects. 7. Potential future actions (if identified)	Assess the impact on rights and freedoms of data subjects. Identify type of information affected, volume of data Record your decision to notify or not to notify. Ensure you record your rationale to not notify. Use your notes taken during the incident.
If applicable inform Data Subjects: - - without undue delay	Assess the impact on rights and freedoms of data subjects. Record your decision to notify or not to notify. Ensure you record your rationale to not notify. Use your notes taken during the incident.
Internal Reporting and Learning - What can we learn from this incident? - Further training or information for staff? - Change to internal practices or procedures?	Create an action plan for delivery of actions within 4-6 weeks. This also provides evidence for decisions made and actions taken.

Appendix B: Data Breach/Loss Report (Actual/Near Miss)

Data Breach/Loss Incident Report	
Report by:	Date of Report:
Date of Incident:	Actual or Near Miss:

Internal

Details (provide details of incident, actions taken to mitigate, further action required)
Circulation