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

- Accountability: Commissioner
- Oversight: COO and Deputy Commissioner
- People and Culture Lead Change Maker for staff data
- Head of Finance for financial data
- Data Protection Officer (DPO): Finance and Corporate Governance Officer
- Claire Rees for comms data
- All staff and associates are required to comply with this policy.
- **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
- Devices 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 Sang-Jin or COO Marie 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 Commissioner's senior staff team to the Commissioner and their 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. We also use reputable software/platforms such as PeopleHR and Sage.

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 with 2-factor authentication and strong passwords. Most of our devices have fingerprint or facial recognition technology to unlock the devices.
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 done by landlord.
4. Client devices managed by Orbits are protected by antivirus and security software (Webroot).

5. Standard users have no administrator access to devices. Only Orbits have administrator rights on 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, Natalie Jenkins or Marie Brousseau-Navarro.

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 immediately Sang-Jin or Susan, and possibly senior staff of breach/loss	Note date and time of breach Note any actions taken *Joint data controllers have joint liabilities in the event of a breach*

3. Check immediately with staff to ensure no unauthorised action that could impact on the breach/loss is taken	
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 to complete the data breach form
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.
Use the data breach form to communicate the issue	Use or template and complete it carefully Share it with SLT and agree communication plan
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)

Report a personal data breach (ICO form)

Please do not include any of the personal data involved in the breach when completing this form. For example, do not provide the names of data subjects affected by the breach. If we need this information, we will ask for it later.

If you have already spoken to a member of ICO staff about this breach, please give their name:

About the breach

What has happened?

Tell us as much as you can about what happened, what went wrong and how it happened.

Was the breach caused by a cyber incident?

- Yes
- No
- Don't know

How did you find out about the breach?

When did you discover the breach?

Date:

Time:

When did the breach happen?

Date:

Time:

Categories of personal data included in the breach (tick all that apply)

- ☐ Data revealing racial or ethnic origin

- ☐ Political opinions
- ☐ Religious or philosophical beliefs
- ☐ Trade union membership
- ☐ Sex life data
- ☐ Sexual orientation data
- ☐ Gender reassignment data
- ☐ Health data Basic personal identifiers, eg name, contact details
- ☐ Identification data, eg usernames, passwords
- ☐ Economic and financial data, eg credit card numbers, bank details
- ☐ Official documents, eg driving licences
- ☐ Location data Genetic or biometric data Criminal convictions, offences
- ☐ Not yet known Other (please give details below)

How many data subjects could be affected?

Categories of data subjects affected (tick all that apply)

- ☐ Employees
- ☐ Users
- ☐ Subscribers
- ☐ Students
- ☐ Customers or prospective customers
- ☐ Patients Children
- ☐ Vulnerable adults
- ☐ Not yet known Other (please give details below)

Potential consequences of the breach

Please describe the possible impact on data subjects, as a result of the breach. Please state if there has been any actual harm to data subjects

What is the likelihood that data subjects will experience significant consequences as a result of the breach?

- ☐ Very likely
- ☐ Likely
- ☐ Neutral – neither likely nor unlikely
- ☐ Unlikely
- ☐ Very unlikely
- ☐ Not yet known

Please give details

(Cyber incidents only) Has the confidentiality, integrity and/or availability of your information systems been affected?

- ☐ Yes
- ☐ No
- ☐ Don't know

(Cyber incidents only) If you answered yes, please specify

(Cyber incidents only) Impact on your organization

- ☐ High – you have lost the ability to provide all critical services to all users
- ☐ Medium – you have lost the ability to provide a critical service to some users
- ☐ Low – there is a loss of efficiency, but you can still provide all critical services to all users
- ☐ Not yet known

(Cyber incidents only) Recovery time

- ☐ High – you have lost the ability to provide all critical services to all users
- ☐ Supplemented – you can predict your recovery time with additional resources
- ☐ Extended – you cannot predict your recovery time, and need extra resources
- ☐ Not recoverable – recovery from the incident is not possible, eg sensitive data has been shared publicly
- ☐ Not yet known

If there has been a delay in reporting this breach, please explain why

Taking action

Describe the actions you have taken, or propose to take, as a result of the breach

Include, where appropriate, actions you have taken to fix the problem, and to mitigate any adverse effects, eg confirmed data sent in error has been destroyed, updated passwords, planning information security training.

Have you told data subjects about the breach?

- ☐ Yes, we've told affected data subjects
- ☐ We're about to, or are in the process of telling data subjects

- ☐ No, they're already aware
- ☐ No, but we're planning to
- ☐ No, we've decided not to
- ☐ We haven't decided yet if we will tell them or not
- ☐ Something else (please give details below)

Have you told, or are you planning to tell any other organisations about the breach?

eg the police, other regulators or supervisory authorities. In case we need to make contact with other agencies

- ☐ Yes
- ☐ No
- ☐ Don't know

If you answered yes, please specify

About you

Organisation (data controller) name

Registered organisation address

Person making this report

In case we need to contact you about this report

Name:

Email:

Phone:

Data protection officer

Or the senior person responsible for data protection in your organisation

- ☐ Same details as above

Name:

Email:

Comisiynydd Cenedlaethau'r Dyfodol Cymru
Future Generations Commissioner for Wales

Phone:

Sending this form

Send your completed form to casework@ico.org.uk, with 'DPA breach notification form' in the subject field, or by post to:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on 0303 123 1113 (operates 9am to 5pm Monday to Friday).