IT Security Policy

Policy Statement

The Office of the Future Generations Commissioner (OFGC) provides systems and hardware to support staff in carrying out their roles.

The Commissioner expects all staff and authorised users of OFGC systems to comply fully with this and other associated policies.

Any non-compliance may be subject to disciplinary action.

Our IT systems are regularly monitored to ensure any risks that may compromise the security and integrity of our systems are identified and dealt with.

Specific breaches may be reported to the police and/or Information Commissioner's Office (ICO).

All staff expected to carefully read this policy, to especially note key points of Acceptable Use and sign to indicate acceptance of terms of use systems and hardware.

Policy Purpose

- To establish standards all staff and authorised users are expected to follow
- To take a balanced and proportionate approach to manage the risk of systems and hardware being compromised (by cyber- attack, malicious or accidental action/non-action)
- To support compliance with FOIA, DPA, Equality Act, Computer Misuse Act
- To ensure appropriate policy and procedures are in place to manage any incidents
- To ensure our business critical technology is resilient and support recovery plans

Roles and Responsibilities

Staff and associates with specific responsibilities in relation to this policy

All staff and associates are expected to comply with the requirements of this policy and to report issues identified in the course of their work with the OFGC systems (e.g. you have access to areas of Sharepoint that your role does not require).

While the Commissioner has overall responsibility for all aspects of organisational compliance, operational responsibility is delegated to individual Directors, Office Manager, Finance and Governance Officers.

Name	Role
Susan Crutcher	Office Manager
Sang-Jin Park	Finance and Governance Officer
Helen Verity	Director of Corporate Governance

IT Support Services are provided by Orbits IT, an external supplier under contract and service level agreement (SLA).

Reporting

Any issues or problems that may compromise system stability or security should be reported in the first instance to Orbits IT immediately (029 20 003313 or helpdesk@orbits.co.uk) and inform the Office Manager as soon as possible. Any IT Security incidents (including data breaches/ losses) will be regularly reported through the Commissioners senior staff team to the Commissioner and her Audit Committee.

Associated Policies

Data Breach Policy

Information Security

Business Continuity Policy

Introduction

Our IT systems are key to how we work efficiently and effectively. But our IT security can be compromised in a number of ways; through external malicious attack (cyber-attack), or by accidental or malicious action within the organisation. Our IT systems are protected and monitored so that external threats are identified and responded to promptly. However, it is often the action (or non-action) of staff within the organisation that can be the most significant threat to IT security.

The following information and guidance is designed to help all Commissioner's staff to use our IT systems and hardware and minimise the risks to IT security.

At the end of this document you will be asked to complete a declaration, you will be required to repeat this annually or if IT systems undergo significant changes.

If you have any queries about this policy and declaration or if there are any related issues or concerns you wold like to raise please contact the Office Manager in the first instance.

Data Breaches/Losses

A data breach or loss can happen as a result of cyber-attack, failure of physical security, loss of hardware, but most often occurs as result of human error. Our Data Breach Policy sets out the actions we should take should a breach occur.
The General Data Protection Regulation comes into force 25 May 2018 and both widens the definition of the term 'breach' and requires organisations to report data breaches/losses to the Information Commissioner's Office and data subjects within 72 hours.

Data breaches can have a significant impact on individual data subjects and can also impact on public confidence in our organisation. We mitigate the risk of data breaches or loss by ensuring that we do not compromise our IT systems or any personal or corporate information held by following the requirements of our
IT Acceptable Use Policy and Guidance.

Acceptable Use Policy & Guidance

IT Systems and Hardware

This policy is designed to ensure that staff and associates are supported to use the OFGC systems and hardware. By following this guidance you will play your part in ensuring secure use of the OFGC IT systems and minimising risks of data loss.

The 'must nots'

- You must not change data structure of any part of the OFGC systems
- You must not deliberately introduce any virus, worm, malware or nuisance programme.
- You must comply with Password Guidance and any requests to change passwords.
- You must ensure that your use of the OFGC IT systems is consistent with our IT Security Policy.
- Software – you must not add any software or applications without express permission of the Office Manager and Orbits.
- Internet access (gambling, pornography sites)
- Network monitored – unacceptable use reported?

- If you are uncertain about any aspect of your use of hardware or systems you should seek advice from Orbits IT or the Office Manager.

Guidance

Passwords - are a first line of defence to prevent unauthorised access to Commission systems and data.

- Ensure you follow the OFGC requirements in constructing passwords
- Never share passwords even with colleagues or family members
- Do not leave password on a post it with your computer, laptop, tablet or phone.
- Always keep your passwords confidential, and avoid using words that are too obvious or may be related to you. Our IT system will automatically require you to change your passwords regularly (every 90 days). Passwords are required to be a mix of at least seven letters, numbers and symbols, to include three of the following four categories:
  Upper case letters (A - Z)
  Lower case letters (a - z)
  Digits (0-9)

Symbols that are not in alphabetical order (e.g.!, $, #,%)

Portable devices (e.g. Laptops, tablets, mobile phones) – Staff are provided with portable devices to support remote working and flexibility. If using any portable devices please ensure you follow the guidelines provided. * Guide to Using Portable Devices.

All portable devices are protected by encrypted software and multi- layer passwords. You should not take any actions that may bypass or undermine this.

Portable media (e.g. data sticks, external hard drives) Data should not be transferred to portable media unless there is a specific business reason to do so. If you wish to transfer data you will need written permission to do so from the Director of Corporate Governance.

Since all our data is retained in cloud services there is a risk that data stored on a portable drive is not secure or backed up.

Mobile and remote use – secure channels and firewalls are in place to ensure data is saved and protected. You should not take any actions that may bypass or undermine this.

Personal use - the Commissioner allows staff to use OFGC systems and hardware for limited personal use. This includes access to social media, internet, shopping and banking. However, as noted above, you must not download software, applications or make any other modifications to IT hardware without the explicit permission of Orbits IT and the Office Manager.

Breaches or losses – hardware (e.g. tablet, laptop, phone or potable media) or information (or suspected loss) must be reported immediately to Orbits IT and the Office Manager. We ask you to report an incident promptly because we may be able to take action to minimise any loss or the impact of a loss.

Our Data Breach Policy sets out the actions to take should a possible breach or loss occur.

User accounts and access control – Access arrangements are monitored and reviewed regularly to ensure access is appropriate

All users are required to report access issues if inappropriate to their role or grade.

IT Equipment Loss, Damage, Disposal

Hardware - Loss or Damage

Any loss of or damage to hardware provided by the Commissioner for your work use (e.g. tablets, phones, laptops, PCs) should be reported immediately to the Office Manager.

This is to ensure any risks of data loss or unauthorised access to corporate information are dealt with promptly.

Hardware – Safe Disposal

If IT hardware is faulty this should always be reported immediately to the Office Manager who will take the appropriate action.

Please note, you should not try to apply fixes yourself.

If hardware is no longer fit for use it will be disposed of safely, ensuring any traces of personal and corporate data is fully removed from the device. The Office Manager is responsible for ensure safe/secure disposal.

Email System Use – Guidelines

The OFGC email system is provided to staff and associates to support their work. The Commissioner expects that all staff and associates use the system appropriately.

You should not compromise our IT system by circulating emails containing unidentified attachments or defamatory, offensive or pornographic material.
This type of action will be investigated and may be subject to disciplinary action.

Retention of emails – in order to manage the volume of data generated through our email system a retention period of one year (from the send date) has been applied. This means that messages older than one year will be deleted from your email folder.

Regular housekeeping – best practice guidelines encourage regular housekeeping of your email account. Please think about retaining important emails or content in other parts of the OFGC system (i.e. outside the email system)

Creating and Forwarding Emails – One of the most common causes of a personal data breach is by human error. For example, an email containing personal information is forwarded 'send to all'. As a creator of email you are data owner, consider the contents and if it should not be forwarded make this clear. It is your responsibility to tell recipient what to do/not do with the email. You can do this by adding a clear instruction in the first line of the message, e.g. Message contains Personal data – do not share outside the organisation without checking with me.

Freedom of Information Act (FOIA) – the OFGC is subject to FOIA and potentially makes any information held by us releasable into the public domain.

This includes information in hardcopy formats (e.g. notebooks, drafts, post it notes) as well as electronic records including email, text messages.

Please note – any work related emails on personal email accounts are subject to FOIA.

If you have any queries about any aspect of this policy and guidance please contact the Finance and Governance Officer.

Declaration

IT Security Policy & Acceptable Use Guidelines

I confirm that I have read this policy and guidance and agree to comply with its requirements.

I acknowledge that my use of Commission systems may be subject to monitoring and that I am required to report any access issues or data losses immediately.

Name Role

Date

Sign

Office use only

Re-declaration due date: