Cyber Security Policy

Inspired Learning Group

August 2024

Contents

1 Introduction

1.1 This policy outlines the guidelines, procedures, and responsibilities for ensuring the protection and security of digital assets, information systems, and data within the group of schools. It is designed to minimise risks and vulnerabilities, maintain confidentiality, integrity, and availability of information, and safeguard against unauthorised access, disclosure, alteration, or destruction of sensitive data.

1.2 The aim is to ensure that appropriate technical and organisational measures provide a level of security appropriate to the risk, including the following as appropriate:

- The encryption of personal data;
- The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- The ability to restore and the availability and access to personal data in a timely manner in the event of a physical or technical incident;
- A process for regularly testing, accessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

1.3 Cyber security is the responsibility of everyone at ILG, and it is important to read and understand the relevant policies.

1.4 A cyber security incident can have a major impact on any organisation and for extended periods of time. For ILG settings and Head Office, this can range from minor reputational damage and the cost of restoring systems from existing back ups, to major incidents such as losing pupils' work or access to learning platforms and safeguarding systems.

2 Application

2.1 This policy applies to all staff working at ILG (whether directly or indirectly), whether paid or unpaid, whatever their position, role or responsibilities, which includes employees, contractors, peripatetic teachers, agency staff, work experience / placement students, apprentices and volunteers.

2.2 This policy is for internal use only, not for publication on any of our websites. This policy can be found on Sharepoint under ILG Head Office External - Documents\GDPR\Policies. It is also available on request from the setting or Head Office.

2.3 This policy applies to all settings within the group and Head Office, and covers all digital systems, networks, software, hardware, and data held by or accessed through these means.

3 Roles and responsibilities

3.1 Management:

- Senior leaders within the settings and Head office will promote a culture of cyber security awareness and allocate appropriate resources for implementing and maintaining effective security measures. They will ensure compliance with relevant laws, regulations and industry best practices. Additional advice may also be provided from Head Office.

- Senior leaders within the settings and Head Office are responsible for ensuring that their staff are trained accordingly.

- The ILG IT lead will oversee and manage cyber security initiatives, including any related risks and control measures for mitigation. They may also instigate additional training or awareness programmes that may be required.
- An insurance policy is in place for cyber security.

3.2 All staff within settings and Head Office are required to:

- Adhere to this policy and report any suspected or actual security incidents immediately to the SLT within the settings or managers within Head Office, or the data protection or ILG IT lead.
- Participate in cyber security training and awareness programmes to enhance their understanding of security threats, best practices and incident response procedures.
- Apply security updates and patches promptly and maintain strong passwords for their accounts.
- Follow data handling and data privacy guidelines, especially when dealing with sensitive information.
- Consider if an email could be a phishing or scam email. If suspected, do not open but forward to the IT Department. Be aware of the common signs:
    - Suspicious sender address. If something does not feel right, check with the sender by another method, particularly in relation to financial transactions, attachments or links to websites.
    - Email addresses and domain names that do not match.
    - Spelling, grammar and layout.
    - Suspicious attachments.
    - Threats or a false sense of urgency.
    - Unusual content or requests – these often involve a transfer of funds, change of bank account which has not been requested, or requests for login credentials.
    - Generic salutations.
- Consider if your account could have been hacked, or that of a colleague. If suspected, inform the IT Department (and colleague if applicable). Be aware of the following indications:
    - Your email has been sending messages you didn't create.
    - Your passwords have changed without you knowing.
    - Your device is installing software that you didn't request or authorise.
    - You get fake antivirus messages asking you to install.
    - Your personal data is leaked.

4 Access control

4.1 User access:

4.1.1 Access to systems, networks and data should be granted on a need-to-know and least privilege basis.

4.1.2 Each user must have a unique user ID and password for authentication.

4.1.3 Strong passwords must be implemented, including regular password changes.

4.1.4 Access rights and privileges should be regularly reviewed and updated to ensure appropriateness, and access revoked for employees or personnel who have left ILG or no longer require it.

4.2 Remote access:

4.2.1 Remote access to systems and data should only be granted through secure and encrypted connections.

4.2.2 Remote access accounts must have unique credentials and use multi-factor authentication wherever possible.

5 Network Security

5.1 Firewalls, intrusion detection/prevention systems must be implemented, and network segmentation considered to protect against unauthorised access, malware and network attacks.

5.2 Network devices, routers, switches and access points must be regularly updated and patched.

5.3 Encryption protocols (eg. WPA2, WPA3) must be used for securing Wi-Fi networks.

5.4 A secure boundary must be maintained between the internal network and the internet to prevent unauthorised access and external threats.

6 Data Protection and Privacy

6.1 Appropriate measures must be implemented to protect the confidentiality, integrity and availability of data.

6.2 Data must be regularly backed up and the integrity of backups verified. The way in which these are done is up to the settings and Head Office.

6.3 Sensitive and critical data must be encrypted as required.

6.4 Data protection and privacy laws and regulations must be followed.

6.5 Consent must be obtained and individuals informed about the purpose of data collection, storage and processing. For the settings, this is done through the publication of the 'Privacy Notice for Pupils and Parents' on their website, and the provision of policies to staff on their intranet. For Head Office staff, this is done through the provision of policies on Sharepoint.

7 Incident Response

7.1 All staff must immediately inform their line manager, or the data protection lead within the setting or Head Office if they become aware of anything which might mean that there has been a cyber

security incident or attack, or if they become aware of a practice that weakens ILG's defences in relation to the protection of data.

8 Security Awareness and Training

8.1 Regular cyber security awareness programmes and training must be conducted for all staff, emphasising best practices, policies and procedures so that they are aware of the risks associated with phishing and other common cyber threats. Training on cyber security for staff is available on the TES platform.

8.2 Similarly, pupils in ILG schools should be educated about cyber security in an age appropriate way.

9 Version control

Date of adoption of this policy	February 2021
Date of last review of this policy	August 2024
Date for next review of this policy	August 2027
Policy owner	ILG Head Office