Isle of Wight
Education Federation

The Governing Board of the Isle of Wight Education Federation

Cyber Security Policy

Author	Mark Overy Josh Collins
Approved by	Full Governing Board
Approval date	January 2023
Review frequency	Annually
Next review	January 2025

Revision History

Revision	Change	Date
0.1	First Draft	22/03/2021
0.2	Minor Amendments	16/04/2021
1.0	Reviewed	29/06/2021
1.1	Adjustment for IWEF and responsibilities	10/09/2021
1.2	Minor Amendments	12/01/2022
1.3	Minor Amendments	16/08/2022
1.4	Minor Amendments	22/09/2022

Contents

1. Introduction

The purpose of this policy is to clearly define requirements for the use of its Information Technology (IT) facilities and its information systems. This is so that users of said facilities do not unintentionally place themselves, or IWEF, at risk. This policy outlines the guidelines and provisions for preserving the security of our Data and Technology Infrastructure. The information within this document is based upon the International Standard ISO 17799 which establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organisation.

2. Scope

This policy applies to IWEF members of staff, students, volunteers and anyone who may have permanent or temporary access to our systems and hardware. The policy is designed to provide protection from internal and external security threats by defining the policy for the protection of the Confidentiality, Integrity and Availability (CIA) of its key data and information along with establishing responsibilities for information security.

3. Objective

Confidentiality - knowing that key data and information can be accessed only by authorised individuals.
Integrity - knowing that key data and information is accurate and up-to-date, and has not been deliberately or inadvertently modified from a previously approved version.
Availability - knowing that key data and information can always be accessed.

4. Policy Elements

4.1 Confidential Data

Confidential data is secret and valuable. Common examples can be, but not limited to, the following:

- Information containing staff, student, parent and governor details.
- Unpublished financial information.
- Contractual data.

All employees are obliged to protect this data and within this policy there will be clear instructions on how to avoid potential breaches/threats and who is responsible for ensuring this. Due to staff having access to valuable, confidential, data, two factor authentication must be in place for these users.

4.2 Personal and Company Issued Devices

Whenever an individual uses their digital device to access Federation emails, accounts or data, they introduce a security risk to said data. Therefore, this policy outlines various guidelines which must be adhered to when it comes to mobile devices to ensure they are secure. These criteria are as follows:

- All devices must be password protected and BitLocker encrypted.
- Personal devices are not permitted to access the Federation’s network, data or accounts. Access to these must only be via company issued devices, such as managed Chromebooks deployed via Google Workspace.
- Company issued devices must only be accessed by the individuals in which the device is allocated to.
- Antivirus must be present and up to date with all point releases and patches.
- Cloud data storage is limited with contextual access rules to ensure availability is only possible when on the physical school sites or via company issued devices externally.
- Accounts should only be logged into via secure, private, networks.
- Attempts to access Public WiFi is not permitted.
- Two Factor Authentication must be in place when accessing organisational accounts for staff.
- Installing extensions and apps, outside of the approved list, is not permitted.

When Company Issued Devices are handed to staff, they must read, agree and sign the Equipment Assignment Form along with the Acceptable ICT Use Form. Copies of all forms can be found within the IWEF E-Safety Policy.

4.3 Keep Emails Safe

Emails are one of the most common forms of phishing attacks, scams or malicious software. To minimise the risk of infection or data theft, we instruct employees to avoid opening attachments and clicking on links when the content is not adequately explained or expected. Users should be suspicious of clickbait files, check names and email addresses of senders to ascertain validity. If an email is considered unsafe, the IT Helpdesk is to be notified immediately.

4.4 Manage Passwords Properly

User separation is in place across the network to ensure that access is only available to the resources relevant to the individual user (i.e. Student/Staff/Governor). Passwords leaks are unfortunately very common and are incredibly dangerous as they can compromise the entire IT Infrastructure. All passwords should be secure so they can't be easily hacked and should remain a secret. As a result, IWEF implements a number of password policies for staff, students and governors.

- Password complexity settings to be in place to ensure passwords must have at least eight characters, including upper and lower case letters and at least one number
- Every 3 months, user passwords will expire and a new one will need to be created that cannot be the same as any previously used
- Writing passwords down is not permitted, nor is sharing them with any other individual
- Network administrator passwords must be changed every seven days

Administrative access to the system must also operate in line with the Principle of Least Privilege. The highest level of global administrator can only log on to the Domain Controller. There is an individual administrator for member server access and a lower level workstation administrator for client/workstation access.

Local administrative users operate Microsoft's LAPS whereby automated randomised password changes operate continuously to prevent lateral movement.

4.5 Data Transfers

The transferring of any data always imposes a risk to both the data itself and the system in which the data is being transferred from and to. Data can be stored either on-site or within cloud platforms, such as hosted MIS subscriptions or Google Workspace. As a result, all users have a responsibility to safeguard this data and ensure the risk of losing/leaking data is minimised. Therefore, various measures need to be in place from both a technical perspective and also an individual usage perspective.

- Employees must avoid transferring sensitive data to/from other devices unless absolutely necessary, such as USB Devices for exams. When needing to transfer en masse, employees must seek support via the ICT Helpdesk.
- Sharing of confidential data is only permitted within the Federation's network or via a company owned device.
- Sharing data held within Cloud Storage (such as Google Workspace) to external parties is not permitted. Should documents need to be transferred, this must be done via secure, password protected, zip files using the organisation's dedicated mailing service.

It's very common to use USB external media, such as Mass Storage Devices or Cameras, to transfer data. However, USB devices are susceptible to breaches especially if used on personal devices and then attempting to connect to the infrastructure on site. As a result, IWEF enforces specific network policies to mitigate this risk. This includes Group Policies to disable USB Media usage for Staff accounts due to their ability to access confidential data. Students, however, have the ability to connect Camera devices to transfer photos and media as part of their coursework.

Should an individual be concerned about a scam, breach or potential threat, the ICT Helpdesk must be notified immediately. This includes active attacks and phishing emails however, it is important to remember not to forward on potentially malicious emails to anyone - notice to the ICT Helpdesk can be either via the telephone or a separate email.

4.6 Network Protection

IWEF are responsible for vast amounts of data, both confidential and network related. Whilst there are many steps outlined in this document that individuals must follow, there are a number of additional services and products that need to be in place to ensure the system, and thus the data, is as secure as possible. Traditional measures would include a Firewall and Web Filtering appliance which handles the traffic coming in and out of the network, along with antivirus software installed on as many devices as possible; such as Servers, Clients, Macs etc.

However, due to the ever increasing knowledge of cyber attackers, organisations are advised to procure more in-depth services to be more proactive and to defend against more intelligent attacks. The services to be provided would include:

- Endpoint Protection Agents that utilise Artificial Intelligence (AI) and Behaviour Monitoring should be distributed wherever possible to conduct in-depth monitoring on both the PC itself and the user.
- Security Information and Event Management (SIEM) technology supports threat detection, compliance and security incident management through the collection and analysis (both near real time and historical) of security events, as well as a wide variety of other event and contextual data sources.
- Managed Detection and Response (MDR) services are often coupled with a SIEM solution to utilise their trained Cyber Security Analysts to understand the logs being obtained and to ascertain the potential threats. MDR solutions also provide human interaction and can physically interrupt a cyber attack on your behalf to protect your systems as well as contacting nominated individuals.

Each of these services provide a more in-depth understanding of the activity taking place within the network at any given time. It is important to ensure that these dashboards are routinely monitored, alerts are being sent and all installed agents are up to date. There are additional products on the market that are available and act as a last resort in the case of a successful attack, these are Ransomware Decryption tools. It's important to have a service available to be actively monitoring file shares and the changes within and be able to suspend user accounts, shut down clients and attempt to decrypt files.

The network and server operating systems are required to go through best practice hardening checklists to ensure all necessary security measures are in place and meet all standards.

4.7 Backups

Unfortunately, we are living in a time whereby cyber attacks are happening more frequently and the knowledge of the attackers are growing day by day, often even quicker than the services' defending against them. As a result, it's important to adopt the mindset of 'not if, but when' in terms of it happening. Therefore, the ability to recover from a successful attack and rapidly continue the service and delivery of education within the classroom is of paramount importance. Moreover, the Federation must ensure that an air-gap backup strategy is in place to contribute to the 3-2-1 backup method. Types of backup that must be implemented are as follows:

- Localised, on-site, backups with file storage and versioning.
- Removable tape storage that utilises a Daily/Weekly/Monthly/Yearly backup routine, often referred to as the Grandfather-Father-Son routine, allows the physical copy of the data to be removed from site and kept in a secure location.
- Uploading backups to a cloud based system, with different Geographical Data Centres, offers a final layer of protection.

Not only is it important to ensure these backup routines are being implemented daily, the IT Department must carry out quarterly 'proof of concept' tests to ensure that the data being backed up is capable of a successful restore should this be needed in the event of an attack. A regular restoration process must be conducted for all methods to evidence that the backup strategies in place are reliable and can be called upon when needed.

4.8 Update and Patching Routine

Operating systems and software will receive regular updates for both feature improvements and bug fixes but most importantly, these updates can often address various vulnerabilities and security issues. As a result, it’s crucial to ensure that time is allocated on a monthly basis to assess the environment for any updates. Predominantly, clients will receive updates via a centralised Windows Update Server which also reports back on the type of files and programs that are receiving updates along with cleanup routines.

In addition to routine operating system updates, localised software installations will need to be regularly assessed for updates and vulnerability patches. Similarly to the client updates, time should be allocated to research the most up to date version of each piece of software in use across the Federation, cross-reference this to the centralised Software Audit log and deploy updates that reference any patches, exploits, vulnerabilities or security enhancements. This centralised log is to be updated each month with the checks taking place along with if an update has been deployed or not.

4.9 Additional Behavioural Measures

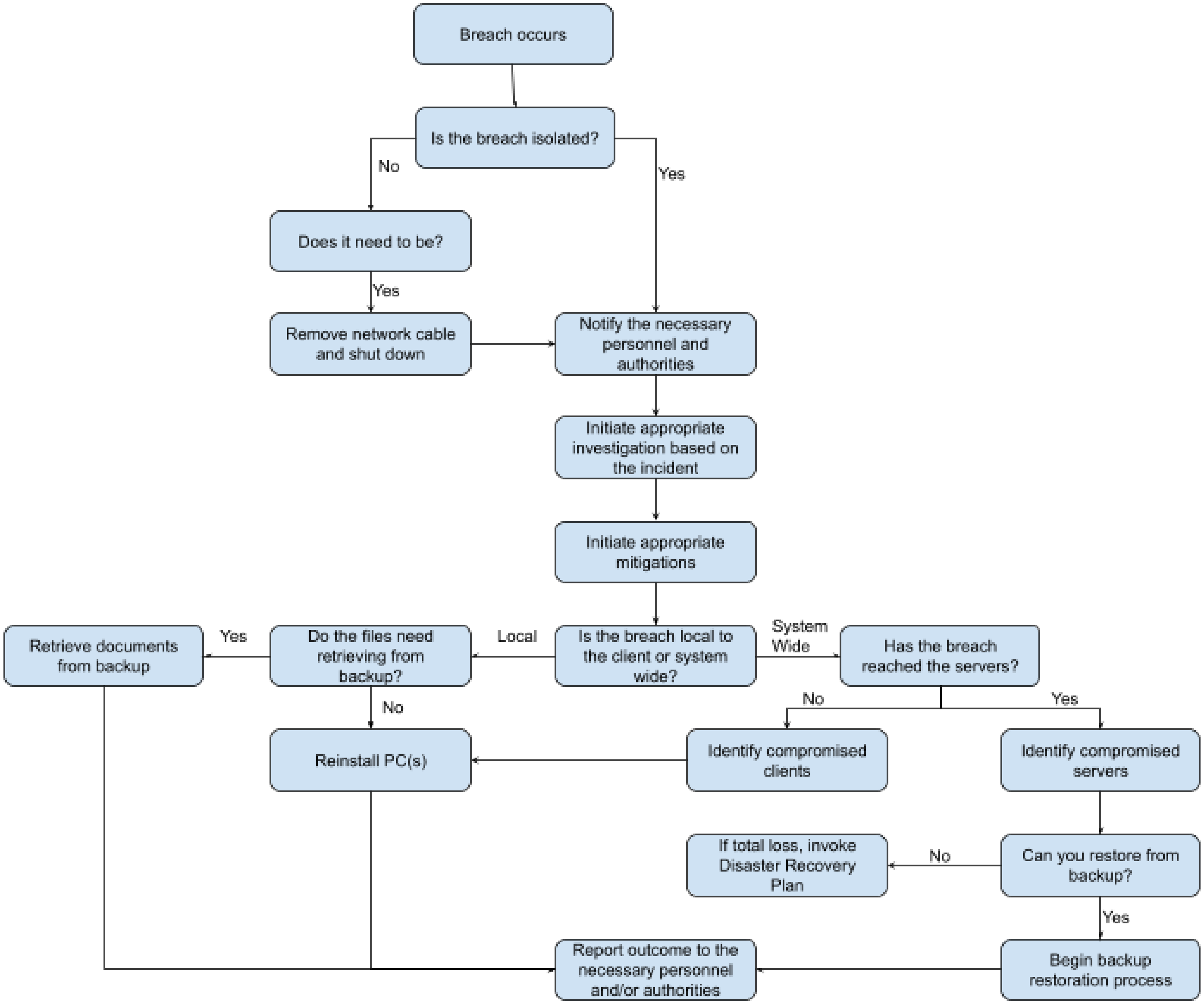
Whilst the IT Infrastructure can be designed to defend against attacks as best as possible, there are numerous behaviours and practices that staff/students/visitors should be following when using the Federation’s IT System. Some examples include:

- When leaving the desk/office/classroom, users should either fully sign out of the device or at a minimum ‘Lock’ the screen temporarily until back in the room.
- Stolen, broken, missing goods should be reported to the ICT Helpdesk immediately. Daily Suite checks take place by the on-site technician, but damage can occur at any point throughout the day.
- Should a device be lost/stolen, all accounts that have been used on said device must have the passwords changed immediately and the ICT Helpdesk should be notified.
- Refrain from visiting untrustworthy sites, especially websites hosted outside of the UK.

4.10 Incident Management

In the event that a breach has been successful, immediate action must be taken. As referenced in Section 4.6, the Network Protection software in place will be reporting against any suspected directions using their various communication methods, as a result the Network Monitoring Team will be notified of all potential breaches. From an end user perspective, should a breach be apparent, the first step will be to network contain the device and if possible shutdown the machine in question. This will allow the IT Management Team to assess any potential damage, data loss or breach movement. In the event that there is localised data loss, be it to the machine Operating System or User Data, using the measures in place outlined in Section 4.7, a recovery attempt will be conducted for data or a reinstallation of the affected device.

Should the initial assessment identify that data retrieval is not possible and the breach has gained deeper access, resulting in a total loss scenario, the Disaster Recovery Plan will need to be followed. Appendix I references a flowchart outlining the process to follow depending on the severity of the incident.


Breach occurs
Is the breach isolated?
No
Yes
Does it need to be?
Yes
Remove network cable and shut down
Notify the necessary personnel and authorities
Initiate appropriate investigation based on the incident
Initiate appropriate mitigations
Is the breach local to the client or system wide?
Local
System Wide
Do the files need retrieving from backup?
Yes
Retrieve documents from backup
No
Reinstall PC(s)
Has the breach reached the servers?
No
Yes
Identify compromised clients
Identify compromised servers
Can you restore from backup?
No
If total loss, invoke Disaster Recovery Plan
Yes
Begin backup restoration process
Report outcome to the necessary personnel and/or authorities

Appendix I - Incident Flowchart

5. Disciplinary Action

The expectation is that anyone accessing the IWEF IT Infrastructure will adhere to this policy and follow best practice, those who cause security breaches may face disciplinary action. A deliberate and serious breach of this policy is likely to lead to the Governing Body taking disciplinary measures in accordance with IWEF's Disciplinary Policy. As per the Acceptable Use Forms held within the e-safety policy, there are strict behaviours which are expected to be followed, likewise there are guidelines on what is not acceptable.

The Federation's phone, web-based and locally hosted systems and email related resources are all provided for business purposes and therefore IWEF maintains the right to monitor all internet and local traffic.

Examples of deliberate or serious breaches of this policy are, but not limited to:

- Knowingly disclose login information to an unauthorised party.
- Inappropriate disclosure of personal information.
- Knowingly installing software on organisational devices that have not been approved by the IT Department.
- Exploiting the use of insecure media such as removable mass storage devices that leads to a breach.

Data security is everyone's responsibility. All IWEF members should feel as though their data is safe and the only way to ensure this belief is to proactively protect our systems and data along with ensuring all users conduct themselves appropriately and in accordance with the AUP and Cyber Security Policy.

6. Safeguarding

Schools have a statutory responsibility to monitor their digital environment to identify any potential threats to pupils' welfare and wellbeing. It's crucial that the schools have appropriate filtering and monitoring in place.

Company owned devices will be continuously monitored for safeguarding risks. If students and staff use a company owned device outside of school, the device will continue to be monitored when it is online and will have the same level of content filtering as if on site.

Monitoring what is blocked by the filter allows schools to identify individuals using inappropriate search terms, so that they can be given advice/support, and to see any trends, which can be used to inform the school's curriculum/advice to staff, pupils and parents/carers. Notifications relating to these inappropriate or concerning web activities are to be automatically emailed to the Designated Safeguarding Leads for further investigation.

In the case of a specific allegation of misconduct, the Designated Safeguarding Lead can authorise access to the specific content of transactions in order to investigate the allegation.

7. Reporting Information

Reporting a potential breach	ICT Helpdesk	helpdesk@iwef.org.uk
Questions relating to this policy	Director of Facilities & ICT	mark.overy@iwef.org.uk
Questions relating to this policy	Operations Manager (Systems)	josh.collins@iwef.org.uk