



**Gilfach Fargoed and Park Primary Schools Federation**

|  |  |
| --- | --- |
| Policy Title: | Schools Procedure for Reporting Cyber Security Incidents and Potential Data breaches |
| Adoption Date: | June 2023 | Review date:  | June 2025 |
| Signed, Chair of Governors:  |  | Signed, Headteacher:  |  |

**Mission Statement**

In our Federation, we are all learners for life. Our schools prioritise authentic, nurturing relationships through which we provide engaging and inspiring learning experiences. We set high-expectations, achievable through the development of resilient and confident learners who have a curiosity and enthusiasm about their community and the wider world. We take a pride in our learning, we thrive on collaboration and we are ambitious to solve problems and to achieve our best. We respect one another and our wider world while valuing our Welsh heritage. We aim to give our learners the tools to succeed in the 21st Century, with the guidance of a strong moral compass. We develop skills and knowledge, while fostering wellbeing and a growth mindset. Our whole community aims to develop:

* Healthy, confident individuals;
* Ethically informed citizens;
* Creative, confident contributors and
* Ambitious and capable learners.

## Cyber Security Incidents

A user may be alerted to a suspected cyber-attack or actual information security incident through several different sources, depending on the type of incident (**see Appendix A for examples)** Often it will not be immediately obvious if an incident has taken place. However, users are advised to proceed with caution and report all instances where they suspect a security breach has occurred.

**Managing cyber security incidents**

The flowchart in **Appendix B** outlines how cyber security incidents should be reported, recorded, investigated and communicated by the School.

Users must report a suspected cyber-attack or security incident to:

**Emergency Contacts**

IT Security – 01443 863224 / 01443 863227

School Support – 01443 866906 / 01443 866910

And log a call to the **IT Service Desk via**

Email: ithelpdesk@caerphilly.gov.uk

Telephone: 01443 864111 (during core hours 8am to 5pm)

This should be done as soon as the incident is discovered so that actions can be taken to mitigate the risks of the incident and put security measures in place to prevent a similar incident from happening again.

A cyber security incident will not always involve personal information, but where personal data is involved, data protection laws will apply.Article 4(12) of the UK GDPR defines a personal data breach as:

*“the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed”*

**If a cyber security incident discovered involves personal data, the school must report the breach of personal data to the Information Governance Officer for Schools.**

Any data breach reported will be assessed on an urgent basis so that a decision can be made on whether we need to inform the ICO within the statutory 72 hours. Therefore, please ensure as much detail as possible is included in the incident report form template and send to Schooldataprotection@caerphilly.gov.uk

**The cyber security incident report should include the following details at a minimum:**

* The full name and contact details of affected user(s)
* The date and time when the incident was observed or suspected
* A full description of what happened and what steps the user undertook
* An outline of the data involved in the cyber security incident (without giving the actual data, unless specifically requested). Please confirm if personal or special category data is thought to be involved. **Data Protection Definitions are included in the grey box below for reference.**
* Does the data just relate to the user in question, or could other user’s data be impacted? If the latter, give an estimate of the likely number impacted (1 – 10, 11 – 100, 101 – 499, 500+).
* A description of the application, system or website in use at the time
* Details of the device involved (i.e. PC, laptop, chromebook, tablet)
* Any other information that might be of relevance

**Data Protection Definitions:**

**Personal data** relates to a living individual, who can be “identified, either directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.” [Article 4(1) of the GDPR]

**‘Special categories of personal data’** [Art 9 GDPR] includes personal data such as:–

* the racial or ethnic origin
* political opinions,
* religious or philosophical beliefs,
* Trade Union membership,
* genetic and biometric data
* health data,
* sexual life or sexual orientation.

Article 10 of the GDPR covers criminal offences and proceedings, including sentencing.

In general, users are not advised to try to resolve such incidents themselves. Instead, report the matter promptly to the IT Service Desk and await a response from the School Support Team. Cooperation with the School Support Team is critical, so users are asked to follow any instructions given to them exactly and promptly.

The IT Service Desk will log the incident as a ticket in the IT Service Management System. All information supplied as part of any investigation will be treated in confidence and handled on a need-to-know basis.

In some cases, a user will not be aware a cyber-attack or security incident has occurred affecting their account and/or data, and will first learn of it when informed by the IT Service Desk or School Support Team with instructions on how to proceed. This will happen in the event a system-generated warning has been triggered.

**Process for responding to a cyber security incident**

The IT Service Desk will review incoming reports of a cyber-attack or an information security incident affecting School systems and/or data. They will log this in the IT Service Management System and it will be assigned to the School Support Team.

The School Support Team will triage the matter to identify the severity and scope of the incident. This will include making an initial assessment (in normal working hours) within 2 hours. However, this timeframe will not always be achievable.

**The School Support Team will consider the following:**

* type of incident
* number of users affected, and any distress caused
* volume and sensitivity of data impacted
* overall effect on School operations, such as the legal or commercial implications.

After analysis, it may be determined that the incident is considered relatively low risk with a known resolution path. The School Support Team will then undertake any remedial measures identified (if any) and close the incident. The affected users will also be informed and given appropriate advice on how to proceed.

Where there is a more serious incident, or where the severity and extent is unclear, the matter will be escalated to the School Support Team Manager, IT Security Team, and Corporate Information Governance Unit (if personal data is involved). An investigation will be carried out and the issue fully documented. This may involve further representations from the user(s) – as well as ensuring all relevant information is gathered and preserved. The School Support Team may also request physical equipment to be submitted for investigation.

If information relating to the incident – particularly that of a personal nature – needs to be recorded, this will be logged in a manner that limits access only to those requiring it.

An impact assessment will be made based on the probable breach of confidentiality, integrity, and availability - the three key elements of information security known as the ‘CAI triad’. The School Support team will consider the impact on wider users and systems as part of the impact assessment. If it proves necessary – for example, there’s a likely impact on the financial wellbeing of the organisation, or possible reputational harm – then the matter may be escalated for a wider incident response. Alongside that, the School Support Team Manager will move to the containment and recovery phase (see below).

Affected users will be kept informed during this process and, where possible, steps will be taken to ensure that disruption to their activities are minimised. For example, by offering the use of temporary equipment or to restore access to the suspected device in a sufficiently short timeframe if not possible.

**Containment and Recovery**

In consultation with the IT Security Team the School Support Team Manager will decide on the appropriate course of action to limit the impact of the incident and mitigate any knock-on effects. School-based staff are expected to give their full support as part of the containment and recovery stage. This may also involve individuals from different departments within Digital Services. This may involve isolating compromised network equipment to create a network firebreak, as well rebuilding/reimaging devices where appropriate.

Consultation with third party organisations may be necessary to undertake the containment and recovery of the most severely affected systems and data.

All steps to recover lost or damaged data will be undertaken to limit the spread, and to attempt to resume normal activities. Where necessary, this may mean restoring from system backups or resetting/recreating compromised accounts. System owners and Information Governance Leads will be informed where assets under their management are likely to have been impacted.

For very serious incidents involving suspected or actual criminal intent, equipment will be seized and securely stored by the School Support Team as evidence for a potential criminal investigation.

Every step undertaken will be documented for audit purposes and, if appropriate, potential future legal action.

**Escalation**

Initial triage of reported security incident will be carried out by the School Support Team. The matter may be escalated to the School Support Team Manager following an initial risk assessment. A decision may be taken to involve the IT Security / Information Governance teams and Cyber Security Forum if it is believed that personal or confidential business data has been compromised, or a significant number of individuals have been adversely affected by the incident.

The Cyber Security Forum would undertake a review of the issue and assess the scope, scale, and impact of the incident. If personal or special category data has been seriously compromised, this will be escalated further to the Corporate Information Governance Unit for investigation. If so, it’s possible that the School Support Team will be asked to impound devices and collect evidence.

The Head Teacher at the school and the Head of Customer and Digital Services in the Authority will be informed following the triage stage. A decision will be made on the proposed course of action. If they declare it to be a major incident, then professional support services, such as HR and the Legal department, will be engaged in accordance with the prescribed major incident procedures.

Issues likely to have a widespread impact on the School and Local Authority as a whole (whether reputational, financial or operational) will be escalated to the Director of Corporate & Education and the Chief Executive. In particular, if a serious data breach is suspected, the Local Authority Legal department may become involved along with the Data Protection Officer (DPO) and their team.

If the scope, scale, and visibility of the issue means there may be outside media interest or a cause for concern amongst business partners or other organisations, then the Communications Unit will be involved in the response.

A personal data breach that is likely to result in a high risk of adversely affecting individuals’ rights and freedoms must be reported to the Corporate Information Governance Unit within 24 hours of becoming aware of the breach, where feasible. The DPO will be responsible for the decision whether the incident needs reporting to the Information Commissioner’s Office (ICO) within 72 hours in accordance with Article 33 of the UK GDPR. They will also handle communications with the ICO and data subjects where notification is required.

Depending on the nature of the security incident, it may also be necessary to inform the Police or other external government agencies such as the [National Cyber Security Centre (NCSC)](https://www.ncsc.gov.uk/scheme/cyber-incidents) . This will be determined by the IT Security team and the Head of Customer and Digital Services.

Consideration will also be given to involving the JISC Cyber Security response team depending on the nature and spread of the issue, especially in the case of a denial of service attack or a ransomware attack.

**Closure and Lessons Learned**

A security incident may be closed only once all containment and recovery activities are complete, and efforts have been exhausted to limit the fallout and impact. A recommendation to close will be made by the School Support Team Manager and will require approval from the IT Security Team or the Head of Customer and Digital Services.

Closure will be noted within the reporting system, along with a final closure report. A closure meeting may be called to confirm the above are complete, and review/conclude any communications with external organisations, such as the ICO.

For serious incidents, and particularly those without precedent, important lessons will need to be learned. This will include a review of the actions taken to determine whether improvements could be made (i.e. how the response could be faster and/or more effective). Steps and measures will be taken to limit the exposure to similar issues in future. This may include hardening defences as well as strengthening operating procedures. All changes and recommendations will be documented against the incident. The IT Security Team is expected to lead this activity in consultation with other staff involved in the incident response.

**Appendix A:**

**Examples of cyber-attacks or security incidents**

There are a wide variety of cyber-attacks or security incidents that users may be exposed to, some of which are potentially serious especially if carefully targeted at an individual or group of individuals. Other attempts are more random and generally easier to identify, but still represent a risk to the organisation and the individual.

Users are advised never to disclose password details or any other authenticating information (e.g. MFA response codes) to anyone claiming to represent the Local Authority or any other associated organisation. A user will never be asked to disclose this type of information from a member of Caerphilly CBC staff.

**The following represent a selection of the most common types of cyber-attacks and attempts to compromise security:**

* **Malware:** This represents any type of malicious or ill-intentioned software that has found its way into a system. Often this is software that’s mistakenly downloaded from a seemingly benign website or installed from an email attachment or link (see also Phishing attempt below). Emails, memory sticks, and other removable storage are also often a source of these.

Malware can often take the form of a virus that attempts to spread itself across a network, harming the host device and/or harvesting confidential information in the process. For example, using key-capture software to collect passwords. The antivirus software installed on many devices should identify and neutralise many of these but is not considered fail-safe. Users should report any instances whether suspected or observed.

One of the most serious types is ransomware. This is software that typically encrypts a user’s data and threatens to wipe it unless a ransom is paid. **If such a program is encountered, a user should never offer to pay the ransom under any circumstances. Ensure the device is disconnected from any network, and then report the issue immediately. This will then be investigated as a high priority matter.**

* **Compromised accounts:** A user account is compromised when someone else gains access to it or makes a deliberate attempt to do so. Once an account is compromised, any data and systems accessed by that user are no longer considered secure.

**An account may be compromised when a user enters their details into a spoofed webpage (i.e. a page that looks genuine to trick someone into giving their account credentials) or by malware that harvests passwords in other ways. If this happens, the user should report it immediately to the IT Service Desk so that the account can be temporarily deactivated and the password reset.**

If it’s clear that data has been accessed and leaked/damaged, then an assessment of the situation will be undertaken and appropriate remedial measures actioned.

Users should be vigilant for this type of attack and users can take steps to prevent such an attack from happening. For example, looking for the secure padlock symbol to confirm a webpage asking for account details is safe to use, and where applicable, using Multi-factor Authentication (MFA) where a SMS code is sent to the user’s mobile phone.

Please be aware that some activities might be classed as cyber-crime under the Computer Misuse Act 1990. These include:

* Using another individual’s username or ID and password to access data, a program, or parts of a system that the user is not authorised to access (even if the initial access is authorised)
* Gaining unauthorised access to school networks, data and files, using computers or other devices
* Creating or spreading computer viruses or other harmful files
* Revealing or publicising confidential or proprietary information (e.g. financial and personal information, databases, computer or network access codes and passwords)
* Disable, impair, or disrupt network functionality using computers/devices
* Using penetration testing equipment without the relevant permission
* **Phishing attempt:** This usually comes via an email that lulls a user into providing confidential information, such as user account information, bank details etc. It may appear to come from a colleague or friend, but this should not be trusted as the friend’s account may already be compromised. The email may ask for the user to reply directly with information (such as a password), or more likely, invite the user to click on a link to a fake or spoofed webpage. It is often accompanied by a chilling warning that failure to do so will result in the account being locked out permanently, or legal proceedings being brought against the individual.

A phishing attempt may also take the form of a phone call or text message purporting to come from a member of staff at the Local Authority, a utility provider, a bank or some other trusted organisation. If genuine, such calls will never ask for confidential information, and will never ask the user to install something on their device. Therefore, if the caller or message is urgently requesting this, it should be treated with extreme suspicion and reported immediately.

**A suspected phishing email received should be reported to the IT Service Desk by sending the suspected phishing email as an attachment rather than forwarding the content.** **This allows the message headers to be inspected. Links and attachments should never be clicked on, and no personal identifiable information should ever be disclosed. If a user believes they’ve inadvertently been lulled into disclosing such information, this must be reported immediately to the IT Service Desk.**

* **Hacking attempt:** This covers many techniques used by criminals to try and overcome security protocols that are designed to protect valuable systems and data. This may include direct hacking attempts to circumvent firewalls, as well as more nuanced attacks, such as Distributed Denial of Service attacks (DDoS) which try to disable a system by flooding them with requests or data.

**Any user who is a victim of such an attempt should report it immediately to the IT Service Desk and mark it as a high priority matter.** Depending on the nature and severity of the incident, it may be necessary for the School Support Team to impound one or more devices for evidence if a criminal investigation is required.

Appendix B: Reporting form

**Cyber Security Incident Report Form**

|  |
| --- |
| **Gilfach Fargoed Primary/ Park Primary****Cyber Security Incident Report Form** |

|  |
| --- |
|  **Incident Information** |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Incident Reference Number |  | Date of incident |  | Time |  |
| Date Reported to school |  | Time |  |
|  |
| Reported by |  | Job Title |  | Phone |  |
|  |
| User(s) affected |  | Location of incident |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Severity\* | High |[ ]  Medium |[ ]  Low |[ ]

|  |
| --- |
| **Details of Cyber Security Incident***Please tell us as much as you can about what happened, what went wrong, and how it happened.*  |
| Describe the Incident*Include how the school became aware of the incident and cause of incident.* |  |
| Describe the application, system, or website in use at the time. |  |
| Please provide details of the device involved – i.e. PC, laptop, Chromebook, or tablet.  |  |

|  |
| --- |
| **Personal Data Placed at Risk (if applicable)** |

|  |  |  |  |
| --- | --- | --- | --- |
| Personal identifiers e.g. name, contact details |[ ]   | Number of individuals affected |  |
| Identification data e.g. usernames, passwords, UPN |[ ]   |  |  |
| Health data |[ ]   | Are the affected individuals aware? |  |
| Data revealing racial or ethnic origin |[ ]   |  |  |
| Religious or philosophical beliefs |[ ]   | Does the data only relate to the user in question, or is other user data impacted? If the latter, give an estimate of the likely number impacted.  | Low (under 50) |[ ]
| Sexual orientation data |[ ]   |  | Medium (51 – 100) |[ ]
| Official documents e.g.  |[ ]   |  | High (101 – 1999) |[ ]
| Genetic or biometric data e.g. fingerprinting |[ ]   |  | Very High (2000+) |[ ]
| Criminal convictions, offence |[ ]   |  | Exact number (if known): |
| Not yet known |[ ]   |  |  |

|  |
| --- |
| **Containment & Recovery***Summarise actions taken to recover from the mistake. Include measures taken to mitigate any possible adverse effects on the individual(s) concerned and actions taken to stop it getting worse, e.g. ‘collected information’, ‘asked recipient to delete it’.* |
| **Action taken to minimise effect on affected individuals.**  |  |
| **Has the data placed at risk now been recovered? Please provide details.** |  |
| **What steps have your organisation taken to prevent a recurrence of the incident?** *Include, where appropriate, actions required to mitigate any further risk (e.g. confirmation data sent in error has been destroyed, changed passwords, planned training)* |  |  |
|  |  |
|  |  |
|  |  |

|  |
| --- |
| **Training & Guidance***INSERT TEXT* |
| **Did the staff members involved in the incident receive training? If so, when?** |  |
| **Please list policies/procedures the School has in place?** |  |

|  |
| --- |
| **For use by Digital Services and Corporate Information Governance Unit:** *The below section is for the School Support team, IT Security, and the contracted Data Protection Officer for schools and their team at Caerphilly CBC to complete.*  |

|  |
| --- |
| **Impact on the UK GDPR (if applicable):** |
| 1. Fairly and transparently processed |[ ]  4. Accurate and up-to-date |[ ]
| 1. Lawfully processed |[ ]  5. Not kept for longer than necessary |[ ]
| 2. Processed for specified purposes |[ ]  6. Organisational security |[ ]
| 3. Adequate for purpose |[ ]  6. Technical security |[ ]
| 3. Relevant for purpose |[ ]  Other |[ ]
| 3. Limited to what is necessary |[ ]   |  |

|  |
| --- |
| **Incident Analysis** – including impact on individuals/risks*Describe the risks or consequences. For example…* |
|  |

|  |
| --- |
| **Corporate action to reduce risk of repeat incident** |
|  |

|  |
| --- |
| **Approval** |

|  |
| --- |
| **Approved By:**The school are advised to review this form after discussing the matter with the contracted DPO and sign to agree with the assessment of risk and recommendations advised.  |
| **Name** |  |
| **Signature** |  |
| **Date** |  |
|  |
| **Closed By:** |
| **Name** |  |
| **Signature** |  |
| **Date** |  |

**Classifying severity of incidents:**

|  |  |
| --- | --- |
| High risk | = incidents that cause a high risk to the individual/authority |
|  | * An incident that causes, or has the potential to cause, severe damage or distress to individuals
* An incident that causes, or has the potential to cause, damage or distress to many individuals
* An incident of such gravity that it involves senior management action
 |

|  |  |
| --- | --- |
| Medium risk | incidents that cause a medium risk to the individual/authority |
|  | An incident below high risk that requires corrective action |

|  |  |
| --- | --- |
| Low risk | = incidents that cause a low risk to the individual/authority |
|  | An incident that needs to be logged and addressed |

**Appendix C: Cyber Security Incident Procedure**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **1. DPA incident suspected** | **2. Prioritise and** **report incident** | **3. Record incident** | **4. Containment****and recovery** | **5. Escalation** | **6. Closure and lessons learned**  |
| Awareness of suspected incident triggered by:* School Staff
* IT Security Team
* School Support Team
* Complaint from a member of public
 | Report incident to their Service Desk as soon as the incident is discovered. **Emergency Contacts**IT Security – 01443 863224 / 01443 863227School Support – 01443 866906 / 01443 866910**And Log a Call to IT Service Desk**ithelpdesk@caerphilly.gov.uk 01443 86411 (8am to 5pm)The IT Service Desk review incoming reports of a cyber security incident affecting School systems and/or data. They will log this in the IT Service Management System and assign it to the School Support TeamIf the cyber incident has resulted in data loss, immediately report incident to:**Information Governance Officer Schools** Schooldataprotection@caerphilly.gov.uk 01443 864049 (8:30am to 5pm)DPO will triage incident to determine whether to report incident to ICO within 72 hours and assess whether reporting breach to data subject is required. | The school will be asked to complete the incident report form and return to the School Support team and/or the Information Governance Officer Schools.Information contained within the form helps us to assess the severity of the incident and decide whether there is a need to involve others in the investigation (e.g. Education IT service).  | IT Security team and School Support Team Manager will decide on the appropriate course of action to limit the impact of the incident and mitigate any knock-on effects.School-based staff are expected to give their full support as part of the containment and recovery stage. This may also involve individuals from different departments within Digital Services.For very serious incidents involving suspected or actual criminal intent, equipment will be seized and securely stored by the School Support Team as evidence for a potential criminal investigation. | Initial triage of reported security incident by the School Support Team. The matter may be escalated to the School Support Team Manager following an initial risk assessment. A decision may be taken to involve the IT Security / Information Governance teams and Cyber Security Forum if it is believed that personal or confidential business data has been compromised, or a significant number of individuals have been adversely affected by the incident.  | A recommendation to close will be made by the School Support Team Manager and will require approval from the IT Security Team or Head of Customer and Digital Services. Closure will be noted within the reporting system, along with a final closure report. A meeting may be called to confirm the above are complete and review/conclude any communications with external organisations, such as the ICO. |