Cyber Security Threats Procedure

Contents

1. Introduction

This document applies to everyone who undertakes duties on our behalf (including third parties, suppliers, partners, and contractors etc.). We have a duty to ensure that the information we process, and hold, is secure. We will react appropriately to any actual or suspected cyber threats relating to information, systems, and data.

We recognise there are risks associated with securing, storing and processing information to conduct our business and have in place Policy and Procedures which need to be followed. Cyber Incidents usually occur when those policies are not followed. Therefore, there is a need to report threats to manage the risks and identify improvements to decrease the number of future Incidents.

Where an external supplier has reported a cyber threat, it is the responsibility of the school to report the threat/breach to the Information Commissioner's Office (ICO), National Cyber Security Centre (NCSC), Police and Action fraud where it meets the threshold to do so.

2. Quick Reference Guide to activities for managing a Cyber Security threat.

- Report the threat to the school office/IT Support, your IT Support should be easily contactable for all school staff via an email address or portal.
- Use the Data Breach Outcome form (found in D6. Data Breach Procedure) to gather basic information about:
    - what has happened?
    - who is involved?
    - what has been done to manage the breach already? The threats listed in **Appendix B** may help you identify the cause.
- From this information, classify the threat using the criteria at **Appendix A**
- If the risk scoring works out at High or Critical, then escalate to the SIRO providing the Outcome form.
- Ensure the SIRO, IT Support and DPO participate in investigating High/Critical/Medium and escalated threats and collect evidence as required.
- Seek advice on High and Critical incidents from the DPO and your IT Support
- Ensure remedial action is taken within 24 hours to recover unlawful disclosure of personal and special category data.
- Provide advice, support, and intervention as appropriate to each case.
- Inform data subjects (parents/ guardians, employees) where appropriate and always where there is a risk of harm or fraud (see example communications at **Appendix D**)
- Identify and manage consequent risks of the threat.
- Identify expected outcomes, stakeholders and any policies or standards that may have been breached.
- Complete the Data Breach Outcome form (found in D6. Data Breach Procedure) and update your B1 reporting tool tab 'data breaches', category 'Network and Cyber Security'.
- Following completion of the Data Breach outcome form analyse results looking at lessons learnt and implement required actions suggested by your

DPO or IT Support. Review the Cyber Security Checklist (**Appendix C**) to ensure all actions are in place.

- Preserve evidence and maintain an audit trail of events and evidence supporting decisions taken in response to the threat.
- Retain records of all threats as evidence of the how the process works and how you mitigate against them in the future. Examples of threat scenarios should be covered within your disaster recovery and/or business continuity plans outlining the process you will follow for several types of threats.
- Develop and implement an appropriate means of preventing similar threats in the future, a tool that can be helpful is MITRE ATT&CK®. This tool outlines procedure examples, mitigations and detection techniques.
- SIRO and IT Support/manager to regularly review the intelligence sources in **Appendix E** so that the school are prepared for live threats targeting public sector organisations or applications/suppliers commonly used within the public sector.

3. Policy References

This procedure is a requirement of the Data Protection Policy and Data Handling Security Policy.

4. Procedures

What is a Cyber Security Threat?

A **cyber security threat** is an attack targeted at a organisation's systems, employee, network, or data.

See **Appendix B:** Cyber Threat Types for a non-exhaustive but comprehensive list of cyber threats.

Cyber Security Definitions

When researching cyber security, completing training, or even reporting a cyber security incident to the National Cyber Security Centre (NCSC) the following terms are highly likely to appear:

Threat Target is the asset that may be attacked. For example, School email account(s).

Threat Agent/Actor is the person or organisation that create the threat. This could be human or non-human, and the threat may be unintentional or intentional. For example, an organised crime group, employees, or a natural disaster.

Threat Source is a person or organisation that funds the Threat Agent/Actor.

Threat Vector is the method(s) used to attack. For example, Phishing emails.

Payload is the part that enacts the attack. For example, encrypting data.

Exploit is the software or code that takes advantage of vulnerabilities to cause disruption on your computer, network, or systems.

Employee Responsibilities

Anyone discovering a threat, even those they think are low risk, must immediately report it to the school office/IT Support.

No retaliatory action will be taken against any member of staff who reports a cyber threat even from another member of staff in good faith, regardless of the seriousness of the threat or the level of the individual responsible for the threat. Identification of a reporting party who requests anonymity shall be protected to the degree feasible but cannot be guaranteed.

All employees should complete the NCSC cyber security training annually here. This should be recorded by the Data Protection Lead on your B1 reporting tool, 'training' tab.

Investigations

The Headteacher or Data Protection Lead will classify the threat using the classification system in **Appendix A**, and an investigator will be assigned. The Headteacher, as Senior Information Risk Owner (SIRO), will oversee all Medium, High or Critical threats to ensure they can assess and recommend a report to the Data Protection Officer (DPO) for the matter to be considered for notification to the Information Commissioner's Office (ICO), National Cyber Security Centre (NCSC), and Police and Action Fraud if required. The school office should seek advice from the DPO for threats they consider 'Medium' or over. In addition, the school office/SIRO should seek advice from their IT Support for threats they consider 'medium' or above.

Timescales

The ICO is clear that you must report a notifiable breach to them 'without undue delay' and not later than 72 hours after becoming aware of it. If you take longer than this, you must give reasons for the delay.

Although there is no legal requirement, you should report significant incidents to the NCSC and UK law enforcement as they are able to provide support.

Should an employee need to triage a cyber threat the NCSC recommend the following in line with the classifications in **Appendix A:**

Critical or High – 3-6 Hours

Medium – 1-2 Days

Low – 5-7 Days

Reporting to the National Cyber Security Centre (NCSC):

Cyber security incidents can be reported to the National Cyber Security Centre - (Report a Cyber Incident - Report a Cyber Incident - NCSC).

You should only report an incident to the NCSC if you believe your network has been comprised or personal data has been affected by a cyber security threat, examples of these threats are in **Appendix B.**

When reporting the incident there are six sections you will need to complete:

1. Report Details
2. Organisation Details
3. Incident Basics
4. Incident Impact
5. Attack Identifiers
6. Attack Specific Questions

You can also report any phishing emails to report@phishing.gov.uk

You should also be able to report any phishing emails to your email provider i.e. Google or Microsoft.

In the event a cyber security threat leads to a major breach:

The Information Commissioner requires major breaches of Data Protection law to be reported within a statutory timescale. Your DPO will assess the need for notification according to the threshold dictated by the ICO.

It is the SIRO's responsibility to decide whether to report a breach to the regulator, the ICO, after consultation with the DPO.

The ICO state that they require notification of breaches where the breach "is likely to result in a risk to the rights and freedoms of individuals. If unaddressed such a breach is likely to have a significant detrimental effect on individuals – for example, result in discrimination, damage to reputation, economic loss, loss of confidentiality or any other significant economic or social disadvantage". Each case must be assessed on a case-by-case basis and should involve the opinion of the DPO.

If the breach is considered to represent a 'high risk' to the data subject rights (i.e. it is a higher level of risk still than that requiring reporting to the ICO), then there is a further requirement that the data subjects themselves are formally notified by the school. The opinion of the DPO should be considered by the SIRO.

If the ICO is to be notified about the breach, the notification must contain:

- The nature of the breach including the categories and approximate number of the:
  - individuals concerned.
  - personal data records concerned.
- The name and contact details of the DPO or other contact point where more information can be obtained.

- A description of the consequences of the personal data breach
- A description of the measures taken, or proposed to be taken, to deal with the personal data breach.
- The measures taken to mitigate any possible adverse effects.

A notifiable breach must be reported to the ICO under the UK GDPR within 72 hours of the school becoming aware of it. The law recognises that it will often be impossible to investigate a breach fully within that time-period and allows you to provide information in phases; however, the initial notification – if it is necessary to notify - must happen within the timescale.

If the breach is sufficiently serious to warrant notification to the public, the school must do so without delay.

The reasons behind the SIRO's decision whether to notify must be documented on the Data Breach Outcome Report Form and must include consideration of the DPO's opinion.

You may also need to consider contacting the police or action fraud.

5. Advice and Support

If you have any issues over the clarity of these procedures, how they should be applied in practice, require advice about exemptions from the requirements or have any suggestions for amendments, please contact your SIRO or IT Support.

6. Breach Statement

A breach of this procedure is a breach of the Data Protection Policy and Data Handling Security Policy. Breaches will be investigated and may result in disciplinary action. Serious breaches of Policy may be considered gross misconduct and result in dismissal without notice, or legal action being taken against you.

Appendices

Appendix A: Incident Classification with associated threats

The below is the suggested template by the NCSC in relation to scoring cyber incidents. Source - Plan: Your cyber incident response processes - NCSC.GOV.UK

Low Incident

- Minimal, if any, impact
- One or two non-sensitive / non-critical machines affected.
- 10% of non-critical staff affected temporarily (short term)
- Should be triaged within 5-7 Days.

Threats that are not limited to but tend to be associated with this classification as per Appendix B – Payment Fraud, Phishing, Quishing, Smishing and Human Error.

Medium Incident

- 20% of staff unable to work
- Breach of small amounts of personal data
- Low risk to reputation
- Small number of non-critical systems affected with known resolutions.
- Should be triaged within 1-2 Days.

Threats that are not limited to but tend to be associated with this classification as per Appendix B – Payment Fraud, Phishing, Quishing, Smishing, Data Loss, Human Error.

High Incident

- 50% of staff unable to work
- Risk of breach of personal or special category data.
- Noncritical systems affected, or critical systems affected with known (quick) resolution.
- Monetary impact
- May need to contact stakeholders so they can take necessary actions such as contacting their bank.
- Should be triaged within 3-6 Hours.

Threats that are not limited to, but tend to be associated with, this classification as per Appendix B – All of the threats listed.

Critical Incident

- Over 80% of staff (or several critical staff/teams) unable to work.
- Critical systems offline with no known resolution
- High risk to / definite breach of special category data
- Monetary impact
- Threat of identity/payment fraud
- Severe reputational damage - likely to impact school long term.
- Should be triaged within 3-6 Hours.

Threats that are not limited to but tend to be associated with this classification as per Appendix B – All of the threats listed.

Appendix B: Cyber Threat Types

The following is a list of cyber threat examples which fall within the scope of the Policy and this Procedure. This is not an exhaustive list.

Phishing – receiving a suspicious message or email which usually contains a link for you to click.

Quishing – being asked to click on or scan a QR code.

Smishing – receiving suspicious messages via SMS usually contains a link for you to click on.

Spear-Phishing – a phishing campaign that targets a specific person or group of people such as administrators.

Denial of Service (DoS) attack – website or network is targeted with continuous malicious traffic rendering it unresponsive or extremely slow.

Ransomware Attack – files and devices become encrypted meaning you cannot access the data stored on them. Usually this is done in the attempt to receive payment to unlock the encryptions.

Hacking – you can no longer access your account, or you notice unusual activity.

Malware / Viruses – network may become slower and harder to use, data may also be encrypted or deleted.

Payment Fraud – a communication tailored to your school in the hope that you will make a false payment (such as an invoice) usually they are sent through via email.

Zero-Day attacks – a vulnerability in your software or hardware is exploited by an attacker before the developer is aware of the vulnerability.

Human Error – a member of staff mistakenly puts the school at risk of a threat.

Environmental and physical disasters – natural disasters that cause damage or loss of data i.e. fires, floods, wind etc.

Data Loss – information is missing on your network or computer which may be due to a wider threat.

Supply Chain attacks – compromising software or hardware before its deployed to the consumer.

SQL Injections - injects malicious code that are destined for storage in a table or as metadata.

Appendix C: Cyber Security Checklist for Beginners

Cyber Security Checklist.docx

Appendix D: Example Communications
Here is an example of wording for communications relating to a data breach/cyber-attack. You will need to consider the circumstances of your breach when drafting a notification to parents or staff.

Notifying data breaches which involve parents/students/employee's data:

Dear [Parent/student]

I am writing to let you know that your personal data [has/may have] been subject to a recent data breach / & Cyber-attack.

[**Describe the event, what you are doing to ensure this does not recur, what personal data has been breached and any potential harm that may arise for them**. **For example**: As you may be aware, the school was the subject of a cyber-attack which may mean that your data and data about ourpupils and staff held on our network have potentially been comprised. The information held on our network comprises your child's name, address, DOB, medical records, grades, ethnicity, SEN, and reports / Employees contact details, bank details, ethnicity, national insurance number, professional registrations, and performance data (delete as applicable).]

We cannot say for sure if cyber criminals have accessed the data, but we wanted to make you aware so that you can take preventative action should you wish to, for example making your bank aware of this potential breach and being vigilant of any unusual contacts quoting your national insurance number. No organisation, including government departments and banks will use your national insurance number to prove their validity, so please be vigilant.

We are working with the DfE, Action Fraud, a branch of the Police, and the National Cyber Security Centre to investigate this attack. We are also working with IT specialists to improve the security of our network and increase our monitoring capability to try and reduce the likelihood of a further attack.

We apologise that this potential risk to your personal data has arisen and are doing all we can to strengthen our defences against cyber-crime.

If you would like to discuss any concerns this may raise, please let us know.

Appendix E: Cyber Intelligence sources

National Cyber Security Centre - https://www.ncsc.gov.uk/section/keep-up-to-date/reports-advisories

Your local resilience centre - Cyber Security & Resilience Consulting Services

Cert EU - https://cert.europa.eu/publications/threat-intelligence/2025

Microsoft - https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/

FBI - https://www.fbi.gov/investigate/cyber

Action Fraud - https://www.actionfraud.police.uk/news

National Protective Security Authority - https://www.npsa.gov.uk/

The Police - https://www.essex.police.uk/advice/advice-and-information/fa/fraud/online-fraud/cyber-crime-fraud/

IGS Newsletters - https://essexcountycouncil.sharepoint.com/sites/IGSDataProtectionOfficerService/SitePages/Marketing-Expression.aspx

Cyber Security for Schools - NCSC.GOV.UK