

**Recognising and Handling Insider Threats**

Updated September 2021

Version 2.0

**Contents**

[**What is an insider threat?** 3](#_Toc84517855)

[**Types of insider threats** 3](#_Toc84517856)

[**1.** **Malicious Insider** 3](#_Toc84517857)

[**2.** **Negligent Insider** 3](#_Toc84517858)

[**3.** **Compromised Insider** 3](#_Toc84517859)

[**Phishing:** 3](#_Toc84517860)

[**Malware infection**: 3](#_Toc84517861)

[**Credential theft:** 3](#_Toc84517862)

[**Reduce the likelihood of insider threats** 4](#_Toc84517863)

[**Handling Insider Threats** 5](#_Toc84517864)

[**Staff:** 5](#_Toc84517865)

[**Contractors / Suppliers:** 5](#_Toc84517866)

[**Pupils:** 6](#_Toc84517867)

[**Consequences of cyber-crime** 6](#_Toc84517868)

# **What is an insider threat?**

An insider threat is a malicious activity against your school that comes from users who you have given network access too. This could be staff, ex-staff who haven’t had their access revoked (removed), pupils, or less commonly, third parties like governors, contractors, or IT providers with access to the schools physical or digital assets.

While we usually talk about insider threats as malicious, it may also refer to users who unintentionally cause harm by their actions.

# **Types of insider threats**

1. **Malicious Insider** - an employee or supplier who knowingly tries to steal information or disrupt operations.
2. **Negligent Insider** - a user who does not follow school IT procedures, such as not locking a machine, sharing passwords, or saving data to insecure locations. This could be due to ignorance or negligence.
3. **Compromised Insider** - a user whose device has been compromised by phishing, malware, or credential theft.

**Phishing: A** targeted user is contacted via email or text message by someone posing as a legitimate contact and attempting to get the user to divulge sensitive data.

**Malware infection**:Malware is an infection which can come from clicking on a link, downloading a file, or plugging in an infected drive, such as a USB.

**Credential theft: S**tealing usernames and passwords by means of deceiving the user, for example by pretending to be IT support staff offering IT help.

Compromised machines can be used to scan file shares, increase user privileges (access), or infect other systems.

Insider threats are difficult to detect because the user (threat actor) has legitimate access to school systems and data to do their work.

In some cases, abuse of access rights takes the form of someone with privileged access abusing their role. School IT staff and external IT providers have been known to exfiltrate (extract) data, read emails and intrusively monitor users.

Example of insider activities and behaviours:

|  |  |
| --- | --- |
| Digital | Behavioural |
| Obtaining large amounts of data | Attempting to bypass security |
| Sharing data with outsiders | Frequently in the office during off-hours |
| Seeking or saving sensitive data | Displaying disgruntled behaviour |
| Requests for access to sensitive data they do not require | Violating school policies |
| Using unauthorised storage devices | Acting withdrawn or unusually quiet. |
| Data hoarding | Talking openly about damaging systems |
| Emailing data outside the organisation | Looking for new job opportunities or talking of leaving |

# **Reduce the likelihood of insider threats**

* Monitor activity - files and emails.
* Understand where your sensitive data is stored and who have access.
* Maintain a least privilege model, with staff only having access to what they need.
* Deploy robust user management and review user access regularly.
* Co-ordinate HR and IT processes to ensure onboarding and off-rolling are seamless, with starter and leaver processes mirroring each other.
* Train all employees to adopt a data security mindset.
* Communicate policies and procedures effectively, to reduce the chance of negligence.

# **Handling Insider Threats**

## **Staff:**

1. All staff should sign an acceptable use agreement and be aware of IT policy. This should cover password requirements and the need to protect user credentials.
2. For accidental or unintentional breaches staff training should be refreshed. It may be prudent to include *all* staff, depending on the issue.

There may be a need to review security protocols in the case of phishing attacks, malware, or poor cyber hygiene, such as weak passwords.

1. For deliberate or malicious actions staff should be subject to the school’s disciplinary procedures.

Referral to the police is necessary where there have been breaches of the [Computer Misuse Act 1990](https://www.legislation.gov.uk/ukpga/1990/18/contents).

1. If staff have copied, shared, or processed sensitive data, this must be reported to the school’s Data Protection Officer. Reporting to the ICO may also be necessary.

## **Contractors / Suppliers:**

1. In all cases refer to the contract and service level agreement (SLA).
2. Accidental or unintentional breaches are likely to be caused by attacks on the supply chain. Refer to the provisions of the contract requiring the supplier to restore access/services. The level of access and security provisions of the supplier should be reviewed regularly anyway, but certainly in the case of an incident.

Contracts should have non-disclosure stipulations for suppliers likely to be supporting any investigative or recovery functions.

Review the time taken for the provider to alert you. If the supplier was not active in contacting you and only aware when the issue affected your users/services, this may indicate issues in their detection and reporting processes.

1. For deliberate or malicious actions refer to the police. There may also be redress for breach of contract.
2. If sensitive data has been lost from third-party systems, or compromised by contractors, report this to the school’s Data Protection Officer. Reporting to the ICO may also be necessary.

## **Pupils:**

If the insider threat is a pupil, the need to provide access to teaching and learning often makes it difficult automatically disablethe malicious user account.

1. All pupils should sign an **age appropriate** acceptable use agreement, covering password requirements and the need to protect user credentials.
2. Accidental breaches may require a review of the curriculum to ensure pupils are aware of their role in protecting school systems. ([Think U Know](https://www.thinkuknow.co.uk/), [Internet Matters](https://www.internetmatters.org/?gclid=EAIaIQobChMIsc_X9qaa8wIVRkiRBR0whQLiEAAYASAAEgLP1fD_BwE) and [i-vengers](https://i-vengers.org.uk/) have resources to support you with this.
3. For deliberate or malicious actions refer to [Cyber Choices](https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/cyber-crime/cyberchoices):

Cyber Choices aims to:

* Deter individuals from becoming involved in cybercrime and prevent re-offending.
* Educate on the Computer Misuse Act 1990 and the possible consequences of breaking the law.
* Promote legal and ethical cyber opportunities.

It is important that pupils accessing systems inappropriately and/or illegally are educated in their knowledge of cyber-crime and the implications and consequences of breaching the Computer Misuse Act.

1. Make sure to check systems for compromises caused by the attacker. Consider what the user may have bypassed and learn lessons from the way in which access was gained to inform changes to processes/policy.

# **Consequences of cyber-crime**

Cyber-crime is a serious criminal offence and anyone (including young people) committing cyber-crime could face:

* A visit and warning from police or National Crime Agency (NCA) officers
* A Cease and Desist visit from police or NCA officers
* Computers being seized and being prevented from accessing the internet
* A penalty or fine
* Arrest
* Up to life in prison for the most serious offences