Gosford Park Primary School

Cyber Security Incident Plan

Key stakeholders

Admin/Curriculum server IT Support: LinkIT

Data Protection Officer: Syeda Ahmed

IT Technician (internal): Tom Adams

Senior Information Risk Owner/Headteacher: Rachael Allen

Information Asset Owner: See Information Asset and Risk Register

Measures taken to prevent cyber security incidents

- Providing staff with relevant cyber security information for example:
    - https://www.ncsc.gov.uk/files/NCSC_NEN%20cards_PRINT-2.pdf
    - https://www.ncsc.gov.uk/information/cyber-security-training-schools
- Up-to-date Security Software and ensuring all devices are set to auto-update
- Ensuring patches are implemented as and when they are needed
- Conducting regular risk assessments for new software (DPIAs)
- Encryption and data backup and ensuring confirmation of backups are in place
- Ensure vendors and partners maintain high data protection standards
- Applying web-filtering
- Applying up to date firewalls
- Applying up to date anti-virus protection
- Ensuring devices are encrypted
- Ensuring devices are configured to prevent software downloads without administrative approval
- Access rights are set to least privileged access and reviewed regularly

- Maintaining an information asset and risk register
- There are procedures in place for creating, managing and deleting user accounts
- Acceptable Use Policy in place
- Personal data breach procedure in place
- Limiting the use of removable media (e.g. USBs)
- Devices have password protection in place, line with the school's Acceptable Use Policy
- Testing suspicious links in https://global.sitesafety.trendmicro.com/

However, cyber incidents can happen no matter how many steps are in place. Knowing what to do **when** an incident arises is important.

Mitigations

Take steps to mitigate the incident:

- Immediately disconnect the infected computers, laptops or tablets from all network connections, whether wired, wireless or mobile phone based.
- In a very serious case, consider whether turning off your Wi-Fi, disabling any core network connections (including switches), and disconnecting from the internet might be necessary.
- Reset credentials including passwords (especially for administrator and other system accounts) - but verify that you are not locking yourself out of systems that are needed for recovery.
- Ensure that the data has been backed up appropriately
- Notify key stakeholders
- Safely wipe the infected devices and reinstall the OS.
- Before you restore from a backup, verify that it is free from any malware. You should only restore from a backup if you are **very** confident that the backup **and** the device you're connecting it to are clean.
- Connect devices to a clean network in order to download, install and update the OS and all other software.
- Install, update, and run antivirus software.
- Reconnect to your network.
- Monitor network traffic and run antivirus scans to identify if any infection remains.
- Take a lesson learned approach

Involve

Ensure your ICT Lead and IT support provider is involved in the first instance.

The DPO may need to be notified without undue delay where an incident involves personal data.

All Cyber incidents should be reported to the Senior Leadership Team without undue delay.

All severe incidents should also be reported to the Governing Body without undue delay.

Action Fraud may need to be notified: https://www.actionfraud.police.uk/

Consider severity

Severity	Examples
Critical	• 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 sensitive personal data • Financial impact • Severe reputational damage - likely to impact business long term
High	• 50% of staff unable to work • Risk of breach of personal or sensitive data • Non-critical systems affected, or critical systems affected with known (quick) resolution • Financial impact • Potential serious reputational damage
Medium	• 20% of staff unable to work • Possible breach of small amounts of non-sensitive data

Severity	Examples
	• Low risk to reputation • Small number of non-critical systems affected with known resolutions
Low	• Minimal, if any, impact • One or two non-sensitive / non-critical machines affected • <10% of non-critical staff affected temporarily (short term)

Categorise

You should also determine what type of incident you are facing. Some examples include:

- Malicious code: Malware infection on the network, including ransomware (data encrypted and payment requested)
- Denial of Service: Typically, a flood of traffic taking down a website, can apply to phone lines, other web facing systems, and in some cases internal systems.
- Phishing: Emails attempting to convince someone to trust a link/attachment.
- Unauthorised Access: Access to systems, accounts, data by an unauthorised person (internal or external) – for example access to someone's emails or account.
- Insider: Malicious or accidental action by an employee causing a security incident.
- Data breach: Lost/stolen devices or hard copy documents, unauthorised access or extraction of data from the network (usually linked with some of the above).
- Targeted attack: An attack specifically targeted at the business - usually by a sophisticated attacker (often encompassing several of the above categories).

Document

Make sure you record the incident in writing:

- Document using the ‘severity’ and ‘categorise’ headings above
- Document any steps taken to mitigate the risks of the incident
- Document who has been contacted and their comments/actions going forward
- Document from discovery to close down