Parrett and Axe School
Cyber Security Incidents Policy

A security breach is any incident that results in unauthorized access to computer data, applications, networks or devices. It results in information being accessed without authorization. Typically, it occurs when an intruder is able to bypass security mechanisms.

Definitions of a security breach

There are a number of types of security breaches depending on how access has been gained to the system:

- An **exploit** attacks a system vulnerability, such as an out of date operating system. Legacy systems which haven't been updated, for instance, in businesses where outdated and versions of Microsoft Windows that are no longer supported are being used, are particularly vulnerable to exploits.
- **Weak passwords** can be cracked or guessed. Even now, some people are still using the password 'password', and 'pa$$word' is not much more secure.
- **Malware attacks**, such as phishing emails can be used to gain entry. It only takes one employee to click on a link in a phishing email to allow malicious software to start spreading throughout the network.
- **Drive-by downloads** use viruses or malware delivered through a compromised or spoofed website.
- **Social engineering** can also be used to gain access. For instance, an intruder phones an employee claiming to be from the company's IT helpdesk and asks for the password in order to 'fix' the computer.

Staff discovering a security breach

1. The breach, whether discovered on the network or on the school website, must be reported immediately to the Headteacher and the Network Manager by telephone or in person.
2. The infected computer/device must be shut down immediately and remain shut down until they are advised by external IT services that it can be opened.
3. The member of staff must provide as much information as possible; i.e. time incident discovered, location of device affected and any action taken at the time. It may be possible to take a photograph of the screen before the computer is shut down.

What happens next

1. The Headteacher or network manager will contact our external IT services
2. The external IT services will investigate the breach and inform the Headteacher and Network manager of the next steps to recovery and the timescale in which this will happen
3. All staff must support the investigation of the breach. Failure to do so may result in disciplinary action.

The Investigation

The Network Manager and external IT Services will:

1. Speak to the staff member reporting the breach.
2. Record evidence and keep an audit trail of events and evidence supporting decisions taken
3. Inform staff where appropriate

Recovery of the network

The Network Manager and external IT Services will

1. Take the necessary steps to restore the network and any data lost or encrypted.
2. Put in place controls to prevent recurrence
3. Complete an Incident Outcome report
4. Send a report of any data breach to ICO

The Heateacher will:

1. Review the Outcome report

2. Ensure that all staff are aware of the incident and any steps that need to be taken to prevent recurrence.
3. Take disciplinary action if necessary

Review

This plan will be Reviewed by the Governing Body on an annual basis. Should an incident occur the following questions should be asked and the plan amended.

- Consider whether an additional procedure could have prevented the intrusion.
- Consider whether a procedure or policy was not followed which allowed the intrusion, and then consider what could be changed to ensure that the procedure or policy is followed in the future.
- Was the incident response appropriate? How could it be improved?
- Was every appropriate party informed in a timely manner?
- Were the incident-response procedures detailed and did they cover the entire situation? How can they be improved?
- Have changes been made to prevent a re-infection? Have all systems been patched, systems locked down, passwords changed, anti-virus updated, email policies set, etc.?
- Have changes been made to prevent a new and similar infection?
- Should any security policies be updated?
- What lessons have been learned from this experience?

Reviewed by the Resources Committee on 6 February 2024

Date of next review February 2025