Spread your wings, learn new things, fly as high as you can.

Cyber Security Policy and Response Plan

Date written: September 2025

Date agreed and ratified by Governing Body: October 2025

Date of next review: by October 2026

Contents

Introduction and Aims

At Dovecotes Primary School we recognise the risk associated with **cyber security** and the need for all stakeholders to comply and adhere to this policy to ensure minimum level of functionality to safeguard pupils and staff and to restore the school back to an operational standard. The aim of the Cyber Security Policy is to establish systems and controls to protect school from cyber criminals and associated cyber security risks – this policy will outline potential risks associated with use of data, IT infrastructure, systems and networks so that these are mitigated through establishing clear and robust acceptable cyber security guidelines through the **cyber response plan**. Without such a plan, the school recognises that recovery can severely impacted, causing additional loss of data, time, and ultimately, reputation.

The school has invested in technical cyber security measures but, together with this, there is the requirement for employees to be vigilant and act to protect the school's IT systems. Concero together with Online Behaviours under the instruction of the SLT are responsible for supporting the school with cyber security. Disciplinary action may be taken if an employee or user is in breach of this policy. This document is to ensure that in the event of a cyber attack, school staff will have a clear understanding of who should be contacted and the actions necessary to minimise disruption.

Scope

This policy applies to all individuals using the school's IT infrastructure, accessing data, systems and networks used both on and off site associated with the school. This includes staff, pupils, governors and technicians using laptops, hard drives, servers, online communications, etc. This list is not exhaustive. This policy should also be read in relation to the following documentation:

- Safeguarding and Child Protection Policy
- Staff Code of Conduct Policy
- Data Protection Policy
- Digital Safeguarding Policy
- Online Safety/Digital Safeguarding Policy

What is cyber-crime?

This policy Cyber-crime is a criminal activity carried out using computers or the internet, which could include hacking, phishing, malware, viruses or ransom attacks. Potential consequences of cyber-crime which could affect an individual or the school include finances, confidentiality, data protection, potential for regulatory breach, reputational damage, business interruption and structural and financial instability.

Cyber-crime prevention

Given the seriousness of cyber crime, the school takes preventive measures and this policy outlines such systems and strategies in order to mitigate the risk of cyber-crime. Measures put in place relating to technology solutions are as follows:

- Firewalls
- Anti-virus software
- Anti-spam software
- Auto or real-time updates on our systems and applications
- URL filtering using Lightspeed
- Device and user monitoring using SmoothWall
- Secure data back up using OneDrive
- Strong passwords
- Encryption
- Deleting or disabling unused/unnecessary user accounts
- Deleting or disabling unused/unnecessary software
- Disabling auto-run features.

Cyber Security Strategy

In addition to above technological solutions, we recognise the importance of having plans in place In order to mitigate risks associated with cyber security and attacks.

Our aim is therefore that the following strategies are in place:

- Cyber incidence response plan – a plan that reflects our school's needs to responses can happen quickly and damage can be minimised.
- Exercise incident response procedures and respond to and recover from attacks – follow the response plan if such an attack occurs so as to recover quickly.
- Cybersecurity training – annual training for both staff and governors is essential as well as curriculum exposure for pupils to ensure stakeholders are updated with potential risks and how to address these and prevent accidental threats.
- Software updates – software and devices are regularly updated to eliminate vulnerabilities that hackers could exploit.
- Multifactor authentication – a hard drive password as well as system password are required for all laptops and CPOMs uses multifactor authentication.
- Data encryption – Hard drives and work emails are encrypted; USBs should not be used without permission from the Headteacher and these must be encrypted.
- Social media screening – online searches are conducted on prospective candidates to protect the school's reputation and safeguard children.

In addition to these approaches, together with Concero and Online Behaviours, the school will:

- ensure we are operating within the cybersecurity standards
- organise an annual audit
- ensure cybersecurity is an integral part of the curriculum
- keep up to date with cybersecurity training and resources.

Controls and guidance for staff

All staff must read and adhere to the guidance in this policy and will be provided with training at induction and refresher training annually and/or as appropriate, i.e. when there is a change to the law, regulation or policy or when significant new threats are identified or have affected school. All staff must adhere to the following criteria:

- Choose strong passwords as outlined above
- Keep passwords secret
- Not reuse the same passwords
- Not allow other people to access the school's systems using your log in details
- Not turn off or attempt to override any security measures
- Report any suspicious activity or mistake that may cause a security breach
- Only access work systems using devices owned by school
- Not install software on school devices without permission from the Headteacher
- Avoid clicking on links to unknown websites, downloading large files or accessing inappropriate content using school equipment and/or networks
- Avoid opening attachments or clicking links with unexplained content (phishing)
- Be suspicious of clickbait titles, e.g. offering prizes
- Check names/addresses on emails received to ensure they are legitimate
- Not misuse IT systems, e.g. accessing inappropriate, adult or illegal content within school premises or when using school equipment
- Not remove data/equipment from school premises/systems without permission
- Install security updated of browsers and systems as soon as updates available
- Log into school accounts and systems through secure and private networks only
- Not leave devices exposed or unattended.

Breach of this criteria may result in disciplinary action. Additional measures to reduce the likelihood of security breaches include:

- Turn off screens and lock devices when leaving unattended
- Report stolen, damaged or faulty equipment as soon as possible with SLT
- Change account passwords when compromised
- Report a perceived threat or possible security weakness in our systems
- Refrain from downloading suspicious material or software
- Avoid accessing suspicious websites.

Our IT technical services (Concero) will support with the following areas:

- Install firewalls, anti-malware software and access authentication systems
- Inform employees regularly about new scam emails or viruses
- Regular training to keep up to date with new scams or cyber breaches
- Investigate security breaches. Follow this policy's provisions as outlined.

Cyber Recovery Plan – also see Cyber Response Plan

The incident management and recovery plan consists of four main stages:

1. **Containment and recovery**: investigating the breach, utilising appropriate staff to mitigate damage and where possible, to recover any data lost.
    i. Verify the initial incident report as genuine and record on the form.
    ii. In the event of a suspected cyber-attack, IT staff should isolate devices from the network.
    iii. In order to assist data recovery, if damage to a computer or back up material is suspected, staff should not:
        1. Turn off electrical power to any computer.
        2. Try to run any hard drive, back up disc or tape to try to retrieve data.
        3. Tamper with or move damaged computers, discs or tapes.

2. **Assessment of the ongoing risk**: To include confirming what happened, what data has been affected and whether the relevant data was protected. The nature and sensitivity of the data should also be confirmed, and any consequences of the breach/attack identified.
    i. Assess and document the scope of the incident using the risk assessment and impact assessment form.
    ii. Start an action log to record recovery steps and monitor progress.
    iii. Make a decision as to the safety of the school remaining open *in liaison with Local Authority Support Services*.
    iv. Make adjustments to recovery timescales as time progresses and keep stakeholders informed.

3. **Notification**: To consider whether the cyber-attack needs to be reported to regulators (for example, the ICO and National Crime Agency) and/or colleagues/parents as appropriate.
    i. Convene the Cyber Recovery Team (CRT) – see below. Liaise with IT staff to estimate the recovery time and likely impact.
    ii. Identify legal obligations and any required statutory reporting e.g., criminal acts / reports to the Information Commissioner's Office in the event of a data breach.
    iii. Follow the *contacts list in the event of an incident* (listed below), executing the communication strategy, which should include a media / press release if applicable. *Communications with staff, governors and parents / pupils should follow in that order, prior to the media release.*

4. **Evaluation and response**: To evaluate future threats to data security and to consider any improvements that can be made. Where it is apparent that a cyber security incident involves a personal data breach, the School will invoke their Data Breach Policy rather than follow out the process above
    - **i.** Upon completion of the process, evaluate the effectiveness of the response using the post incident evaluation form and review the Cyber Recovery Plan accordingly.
    - **ii.** Educate employees on avoiding similar incidents / implement lessons learned.
    - **iii.** Ensure this plan is kept up-to-date with new suppliers, new contact details, and changes to policy.

All documentation mentioned above can be found in the **Cyber Incident Response Plan.**