HOLYWELL CHURCH OF ENGLAND ACADEMY

Cyber Security Policy

Author	MG Simpson
Responsibility	All staff and the governing body
Effective Date	March 2023
Review Date	March 2024
Approved by Ethos Committee:	March 2023
Storage: (i) Electronic (ii) Hard Copy	(i) School network and on Google Drive / School website (ii) Policy file
Distribution	All staff and governors

Purpose
This cyber security policy outlines our guidelines and provisions for preserving the security of our data and technology infrastructure.

The more we rely on technology to collect, store and manage information, the more vulnerable we become to severe security breaches. Human error, hacker attacks and system malfunctions could cause great damage and may jeopardise our school's reputation or threaten our finances.

For this reason, we have implemented a number of security measures. We have also prepared instructions that may help mitigate security risks. We have outlined both provisions in this policy.

Scope
This policy applies to all our staff, governors, contractors, volunteers and anyone who has permanent or temporary access to our systems and hardware.

Roles and Responsibilities
As managing ICT and e-safety are important aspects of strategic leadership within the school, the Headteacher and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The named ICT and e-safety co-ordinators in this school are:
- Mike Simpson (Headteacher)
- Hollie Lau (Senior Leader – Safeguarding Lead)
- Chris Beeden (Data Protection Officer from School Data Managed: contact@school-dpo.co.uk)
- Matthew Perrett (Partnership Education Ltd [PEL]), Sam Howe (Network Manager from PEL) and ICT Technicians from PEL
- Joseph Burnham (Subject Leader, ICT)

Policy elements
Confidential data is private and valuable. Common examples are:

- Data of students/parents/carers
- Financial data
- Personal information

All staff are obliged to protect this data. In this policy, we will give our staff instructions on how to avoid security breaches.

Threats
A threat if left unchecked, it could disrupt the day-to-day operations of the school, the delivery of education and ultimately has the potential to compromise local and national security.

Types of Threats
a) Cybercriminals and Cybercrime
Cybercriminals are generally working for financial gain. Most commonly, for the purposes of fraud: either selling illegally gained information to a third party, or using directly for criminal means. Key tools and methods used by cybercriminals include:

- Malware – malicious software that includes viruses, Trojans, worms or any code or content that could have an adverse impact on organisations or individuals
- Ransomware – a kind of malware that locks victims out of their data or systems and only allows access once money is paid
- Phishing – emails purporting to come from a public agency to extract sensitive information from members of the public.

b) Hacktivism
Hacktivists will generally take over public websites or social media accounts to raise the profile of a particular cause. When targeted against local government or school websites and networks, these attacks can cause reputational damage locally. If online services are regularly disrupted by cyber-attacks this could lead to the erosion of public confidence in using such services. Hacktivist groups have successfully used distributed denial of service (DDoS – when a system, service or network is burdened to such an extent by an electronic attack that it becomes unavailable) attacks to disrupt the websites of a number of councils already.

c) Insiders
Staff may intentionally or unintentionally release sensitive information or data into the public domain. This may be for the purpose of sabotage or to sell to another party, but more often than not is due to simple human error or a lack of awareness about the particular risks involved.

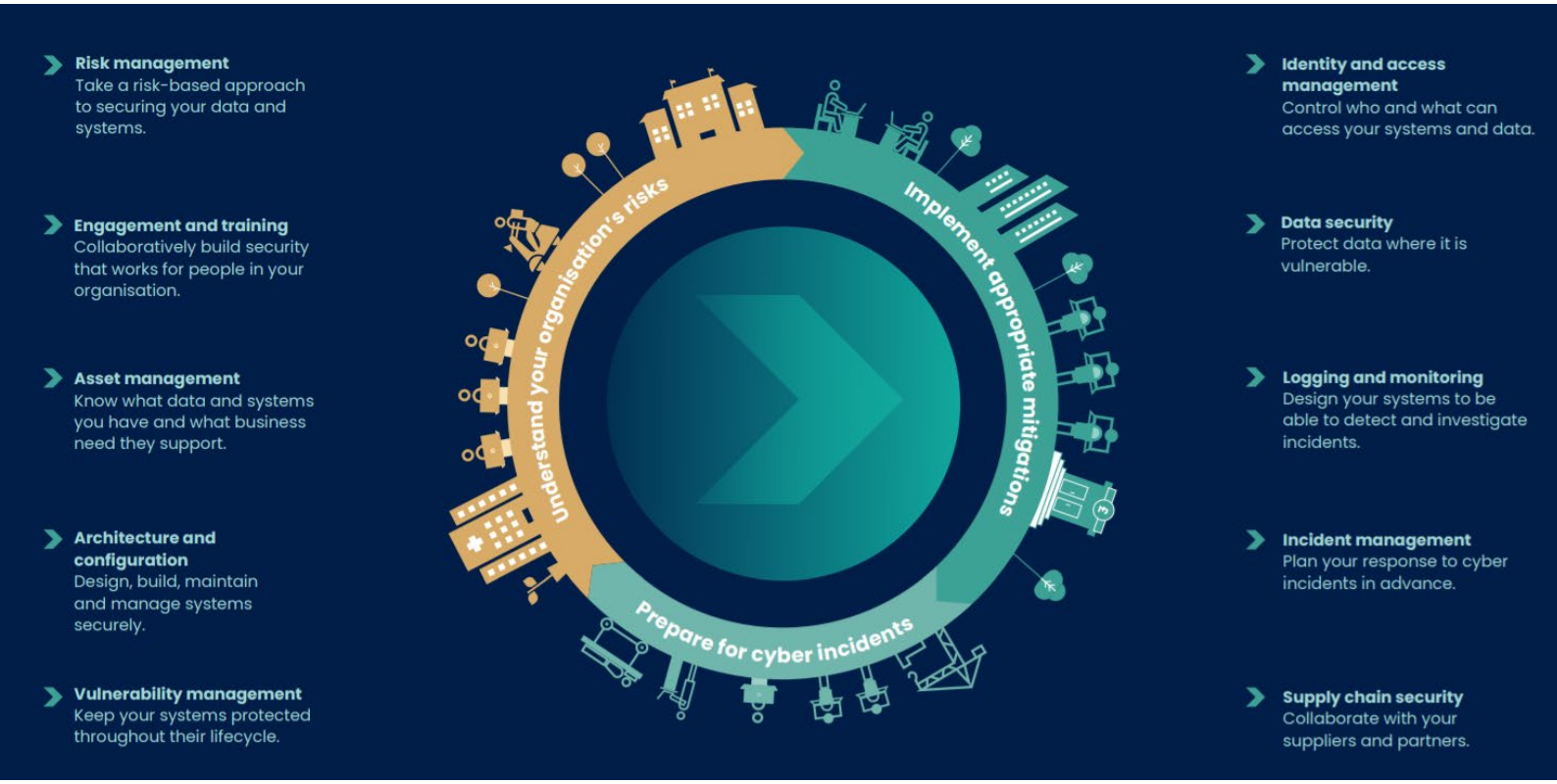
d) Zero-day threats
A zero-day exploit is a cyber-attack that occurs on the same day a weakness is discovered in software. At that point, it's exploited before a fix becomes available from its creator. It is an attack that exploits a previously unknown security vulnerability. This poses a risk to any computer or system that has not had the relevant patch applied, or updated its antivirus software.

e) Physical threats
The increasing reliance on digital services brings with it an increased vulnerability in the event of a fire, flood, power cut or other disaster, natural or otherwise, that impacts upon our IT systems.

f) Terrorists
Some terrorist groups demonstrate intent to conduct cyber-attacks, but fortunately have limited technical capability. Terrorist groups could obtain improved capability in a number of ways, namely through the sharing of expertise in online forums providing a significant opportunity for terrorists to escalate their capability.

g) Espionage
Several of the most sophisticated and hostile foreign intelligence agencies target UK government and public sector networks to steal sensitive information. This could ultimately disadvantage the UK in diplomatic or trade negotiations, or militarily.

10 Steps to Cyber Security
At Holywell, we aim to implement the National Cyber Security Centre's advice for keeping our data secure:



Data and information used
- Student and Staff information in our Management Information System (SIMS)
- Child Protection information (CPOMS)
- Communication – emails and messages through gmail and WEDUC
- Curriculum and Teaching materials
- Records of information (meetings, presentations, etc)

Protect personal and school devices
In general, staff should try to only use school-issued devices to access school emails, accounts or folders. When staff use personal digital devices to access school emails or accounts, they introduce a security risk to our data. We advise our staff to keep both their personal and school-issued computer, tablet and mobile phone secure. They can do this if they:
- Keep all devices password protected.

- Ensure that the school-installed antivirus software (ESET) is installed on their school-owned computer and that they have anti-virus software installed on home computers/devices.
- Ensure they do not leave their devices exposed or unattended.
- Ensure that school-wide security updates of browsers and systems have taken place.
- Log into school accounts and systems through secure and private networks only.

We also advise our staff to avoid accessing internal systems and accounts from other people's devices or lending their own devices to others.

When new staff receive school-issued equipment they will receive instructions for:
- Password management setup

Antivirus / anti-malware software is installed on all school-owned laptops / devices and we advise all staff to have anti-virus software installed on their own devices. .

Staff must follow instructions to protect their devices and refer to our IT Provider – Partnership Education - if they have any questions.

Keep emails safe
Emails often host scams and malicious software (e.g. worms.) To avoid virus infection or data theft, we instruct staff to:
- Avoid opening attachments and clicking on links when the content is not adequately explained (e.g. "watch this video, it's amazing.")
- Be suspicious of clickbait titles (e.g. offering prizes, advice.)
- Check email and names of people they received a message from to ensure they are legitimate.
- Look for inconsistencies or give-aways (e.g. grammar mistakes, capital letters, excessive number of exclamation marks.)
- If a member of staff isn't sure that an email they received is safe, they can refer to Partnership Education.

See the section in the Acceptable Use of ICT Policy for further details on email etiquette and email security.

Manage passwords properly
Password leaks are dangerous since they can compromise our entire infrastructure. Not only should passwords be secure so they won't be easily hacked, but they should also remain secret. For this reason, we advise our staff to:

- Choose passwords with at least eight characters (including capital and lower-case letters, numbers and symbols) and avoid information that can be easily guessed (e.g. birthdays). General guidance on creating a password is to take three random words and to add a number and a special character – eg. DinosaurStarRose14%
- Remember passwords instead of writing them down. If staff need to write their passwords, please keep passwords and identifiers separate or, at least, secure.
- Exchange credentials only when absolutely necessary. When exchanging them in-person isn't possible, staff should prefer the phone instead of email, and only if they personally recognize the person they are talking to.

- Whilst some providers and organisations with whom we work advise (and expect) passwords to be changed regularly, we advise that passwords only be changed if and when they are compromised.

Transfer data securely
Transferring data introduces security risk. Staff must:

- Avoid transferring sensitive data (e.g. customer information, staff records) to other devices or accounts unless absolutely necessary. When mass transfer of such data is needed, we request staff to ask our IT provider (PEL) for help.
- Share confidential data over the school network/ system and not over public Wi-Fi or private connection.
- Ensure that the recipients of the data are properly authorised people or organisations and have adequate security policies.
- Ensure that data is sent to the correct email addresses/contacts and take particular care when sending mass emails (eg. via BCC facility)
- Report scams, privacy breaches and hacking attempts
- Our IT Provider needs to know about scams, breaches and malware so they can better protect our infrastructure. For this reason, we require our staff to report perceived attacks, suspicious emails or phishing attempts as soon as possible to our specialists. Our IT Provider will investigate promptly, resolve the issue and send a schoolwide alert when necessary.

Our IT Team is responsible for advising staff on how to detect scam emails. We encourage our staff to reach out to them with any questions or concerns.

Additional measures
To reduce the likelihood of security breaches, we also instruct staff to:

- Turn off screens and lock devices when leaving desks.
- Report stolen or damaged equipment as soon as possible to ITSupport@holywellschool.co.uk.
- Change all account passwords at once if a device is stolen.
- Report a perceived threat or possible security weakness in school systems.
- Refrain from downloading suspicious, unauthorised or illegal software on school equipment.
- Avoid accessing suspicious websites.

We also expect staff to comply with our social media and Acceptable Use of ICT policies.

Our Security Specialists/ Network Administrators will:

- Install firewalls, anti malware software and access authentication systems.
- Arrange for security training for all staff.
- Inform staff regularly about new scam emails or viruses and ways to combat them.
- Investigate security breaches thoroughly.
- Follow this policy's provisions as other staff do.
- Our school will have all physical and digital shields to protect information.

When working remotely
Anyone working remotely for whatever reason, must follow this policy's instructions too. When staff are accessing our school's systems from a distance, they are obliged to follow all data encryption, protection standards and settings, and ensure their private network is secure.

We encourage staff to seek advice from our IT Administrators.

Reporting incidents, abuse and inappropriate materials
Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the Headteacher. Additionally, all security breaches, lost/stolen equipment or data, virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the school's Data Protection Officer and Headteacher. The school's DPO is Chris Beeden - contact@school-dpo.co.uk.

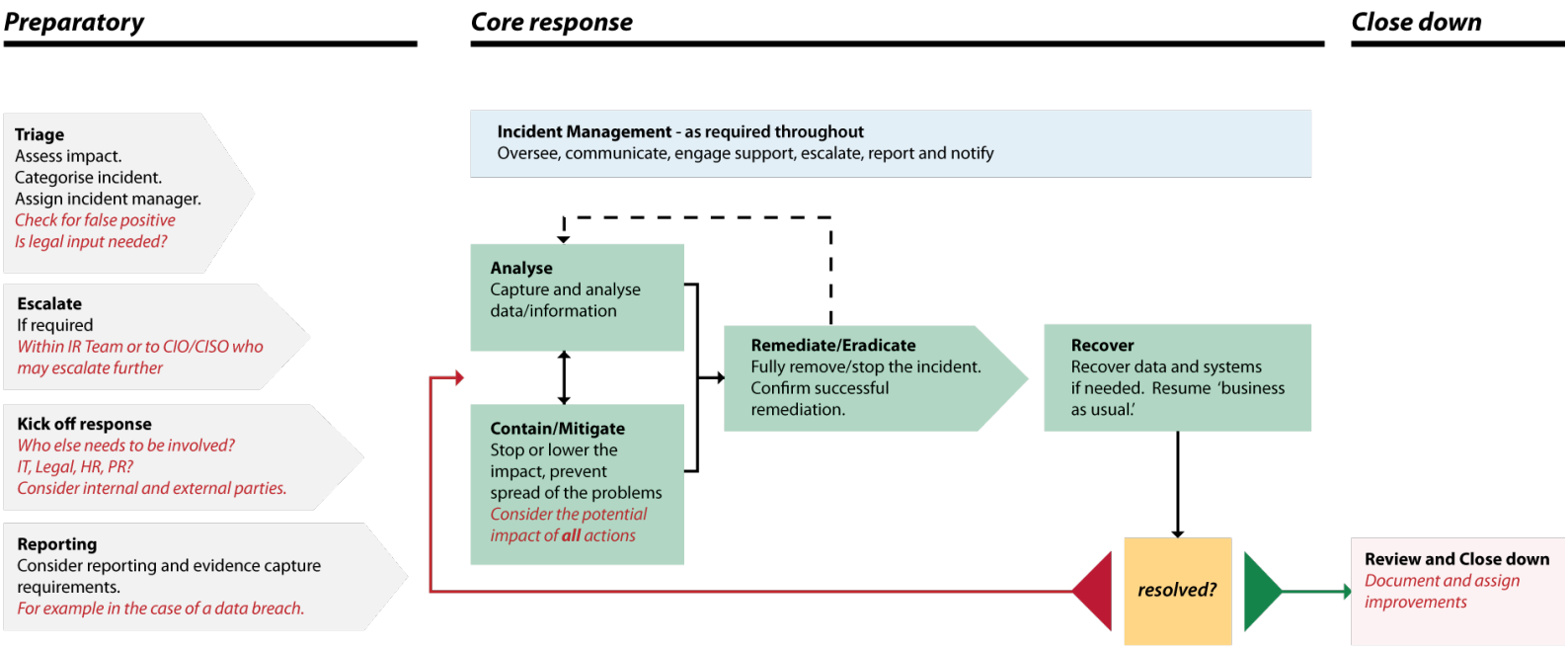
Disciplinary Action
We expect all our staff to always follow this policy and those who cause security breaches may face disciplinary action:

- First-time, unintentional, small-scale security breach: We may issue a verbal or written warning and train the staff on security.
- Intentional, repeated or large scale breaches (which cause severe financial or other damage): We will invoke more severe disciplinary action up to and including termination.
- We will examine each incident on a case-by-case basis.

Additionally, staff who are observed to disregard our security instructions will face progressive discipline, even if their behaviour hasn't resulted in a security breach.

Take security seriously
Everyone, from our customers and partners to our staff and contractors, should feel that their data is safe. The only way to gain their trust is to proactively protect our systems and databases. We can all contribute to this by being vigilant and keeping cyber security top of mind.

Cyber security incident management plan



Inform the local police and education team, National Cyber Security Centre (https://report.ncsc.gov.uk/), Action Fraud (https://www.actionfraud.police.uk/) and Department for Education.