St Cuthbert's
Catholic High School

*Live life in all its fullness*

# Cyber Security Policy

## 2021-2022

| | |
|---|---|
| **Person responsible for Policy:** | Senior Leadership Team |
| **Committee responsible for Policy:** | Quality of Education |
| **Date To Governors:** | September 2021 |
| **Date Agreed:** | September 2021 |
| **Review Due:** | September 2022 and annually thereafter |
| **Is this Policy to appear on school website:** | Yes |

# Introduction

The risk of data theft, scams, and security breaches can have a detrimental impact on school systems, technology infrastructure, and reputation. As a result, St Cuthbert's Catholic High School has created this policy to help outline the security measures put in place to ensure information remains secure and protected.

# Purpose

The purpose of this policy is to (a) protect St. Cuthberts Catholic High School's data and infrastructure, (b) outline the protocols and guidelines that govern cyber security measures, (c) define the rules for school and personal use, and (d) list the school's disciplinary process for policy violations.

# Scope

This policy applies to all of St. Cuthberts Catholic High Schools remote workers, permanent, and part-time employees, students and/or any individuals with access to the school's electronic systems, information, software, and/or hardware.

# Confidential Data

**St Cuthbert's Catholic High School** defines "confidential data" as:

- Unreleased and classified financial information.
- Student and staff information.
- Students and staff passwords, assignments, and personal information.
- School contracts and legal records.

# Device Security

## School Use

To ensure the security of all school-issued devices and information, **St Cuthbert's Catholic High School** employees are required to:

- Keep all school-issued devices, including tablets, computers, and mobile devices, password-protected (minimum of 8 characters).
- Secure all relevant devices before leaving their desk.
- Obtain authorisation from the Head Teacher and/or Business Manager before removing devices from school premises.
- Refrain from sharing private passwords with co-workers, personal acquaintances, senior personnel, and/or students.
- Regularly update devices with the latest security software.

## Personal Use

**St Cuthbert's Catholic High School** recognises that employees may be required to use personal devices to access company systems. In these cases, employees must report this information to management for record-keeping purposes. To ensure company systems are protected, all employees are required to:

- Keep all devices password-protected (minimum of 8 characters).
- Ensure all personal devices used to access company-related systems are password protected.
- Install full-featured antivirus software.
- Regularly upgrade antivirus software.
- Lock all devices if left unattended.
- Ensure all devices are protected at all times.
- Always use secure and private networks.

### Email Security

Protecting email systems is a high priority as emails can lead to data theft, scams, and carry malicious software like worms and bugs. Therefore, **St Cuthbert's Catholic High School** requires all employees to:

- Verify the legitimacy of each email, including the email address and sender name.
- Avoid opening suspicious emails, attachments, and clicking on links.
- Look for any significant grammatical errors.
- Avoid clickbait titles and links.
- Contact the IT department regarding any suspicious emails.

## Transferring Data

**St Cuthbert's Catholic High School** recognises the security risks of transferring confidential data internally and/or externally. To minimize the chances of data theft, we instruct all employees to:

- Refrain from transferring classified information to employees and outside parties.
- Only transfer confidential data over **St Cuthbert's Catholic High School** networks.
- Obtain the necessary authorisation from senior management.
- Verify the recipient of the information and ensure they have the appropriate security measures in place.
- Adhere to **St Cuthbert's Catholic High School** data protection law and privacy policy.
- Immediately alert the IT department of any breaches, malicious software, and/or scams.

# Disciplinary Action.

Violation of this policy can lead to disciplinary action, up to and including termination.
**St Cuthbert's Catholic High School** disciplinary protocols are based on the severity of the violation. Unintentional violations only warrant a verbal warning, frequent violations of the same nature can lead to a written warning, and intentional violations can lead to suspension and/or termination, depending on the case circumstances.

### All users with access to our data are individually known and referenced. Users are only ever granted the level of access required to perform their job. Access and privileges are removed as soon as they are no longer required.

Access and privileges are removed as soon as they are no longer required.
In order to control and audit access to data we need to identify and authenticate every user.

### All users with administrative access to your service are known. Strong authentication and access control is in place for them.

Privileged access may entail logical access to the service, for example through the configuration of operating systems and deployed software packages. But, it could also mean physical access to infrastructure.

Individuals with this degree of access need to be uniquely identified and authenticated with a high degree of confidence.

### All external dependencies (e.g. third-party contractors) which the security of our service and data relies upon are known.

Suppliers are vetted against defined security requirements, supported by contractual arrangements.

Suppliers who operate a service, or part of a service, are often targeted by attackers because of their access privileges.

It is important that we explain our security requirements to our suppliers in a meaningful way, *as well as* ensuring that their contractual obligations reflect our requirements.

## No known vulnerable surfaces are exposed at the edges of our service.

Vulnerabilities in third-party software are mitigated. Custom software - such as web applications - is subject to testing for common vulnerabilities before handling live data.

Continuous testing confirms that all of this remains true.

The vulnerabilities which an attacker can reach first are those exposed by the external interfaces of our service. Typically, these external components would be web applications.
Commodity software components are easily tested for well-known vulnerabilities using vulnerability scanning tools. Custom software - such as our web applications - can also be tested. Using widely available tools it's easy to check for common vulnerabilities such as SQL injection, cross-site scripting, and cross-site request forgery.

## No unsupported software is present in our service and its underlying infrastructure.

Software that is no longer supported will not receive security patches in the event that vulnerabilities become known. This means it will likely be difficult, or impossible, to mitigate any issues that are found.

## Basic attacks against our service would be noticed through proactive monitoring and handled through a measurable, tested, incident response process.

Basic attacks that could be launched by relatively unskilled attackers using widely available tools would be detected by the team operating the service, categorised according to severity, and responded to through a well-known and well-drilled process.

The sort of attacks we would consider 'basic' are:

- attempted DDoS attacks
- attempts to brute force user, service or administrator credentials
- attempts to insert malicious content into a text input field in a web form (SQL injection, cross-site scripting, cross-site request forgery)

Plans are in place to react to attacks against our service. System operators know what action to take, what they *are* authorised to do, and what decisions they would need to escalate.

## All backups or copies of our data are held securely, for the minimum time necessary.

Some of the most high-profile compromises of recent times stole copies (rather than primary versions) of the data from internet-connected services.

We don't hold backups of data on internet-facing services. We archive old records into offline encrypted backups rather than keep them within the online system.

## Ransomware

Ransomware is a type of malware that prevents you from accessing your systems or the data held on them. Typically, the data is encrypted, but it may also be deleted or stolen, or the computer itself may be made inaccessible. Following the initial attack, those responsible will usually send a ransom note demanding payment to recover the data. They will typically use an anonymous email address (for example ProtonMail) to make contact and will request payment in the form of a crypto currency. More recently, there has been a trend towards cyber criminals also threatening to release sensitive data stolen from the network during the attack, if the ransom is not paid. There are many high-profile cases where the cyber criminals

have followed through with their threats by releasing sensitive data to the public, often via "name and shame" websites on the darknet.

## Reducing our exposure using essential security controls

- Boundary firewalls and internet gateways - established network perimeter defences, particularly web proxy, web filtering, content checking, and firewall policies to detect and block executable downloads, block access to known malicious domains and prevent users' computers from communicating directly with the Internet
- Malware protection - establish and maintain malware defences to detect and respond to known attack code
- Patch management - patch known vulnerabilities with the latest version of the software, to prevent attacks which exploit software bugs
- Execution control - prevent unknown software from being able to run or install itself, including AutoRun on USB and CD drives
- Secure configuration - restrict the functionality of every device, operating system and application to the minimum needed to function
- Password policy - ensure that an appropriate password policy is in place and followed
- User access control - include limiting normal users' execution permissions and enforcing the principle of least privilege
- Security monitoring - to identify any unexpected or suspicious activity
- User training education and awareness - staff should understand their role in keeping our organisation secure and report any unusual activity
- Security incident management - put plans in place to deal with an attack as an effective response will reduce the impact on our school

## Storage of data and back-ups

Back-ups of school data are created on a regular basis using an 'offline backup' and remains unaffected should any incident impact our live environment.

With at least one backup offline at any given time, an incident cannot affect all of our backups simultaneously.

These data back-ups are restricted so that they cannot be accessed by staff and are not permanently connected (either physically or over a local network) to the device holding the original copy.

Ransomware (and other malware) can often move to attached storage automatically, which means any such backup could also be infected, leaving you with no backup to recover from. Therefore, we store our backups in a different location, so fire or theft won't result in us losing both copies.