St George’s Primary School
Data Security Policy

Contents

Introduction

This security policy is designed to outline products and practices that will:

- Reduce the risk of a disaster occurring on your school network.
- Protect school data.
- Propose recovery procedures that will get the network back to normal as soon as possible in the event of a disaster.

IT disasters are expensive and time-consuming to resolve. hi-impact aims to pro-actively work with schools to prevent disasters before the need to cure them.

Responsibilities

hi-impact Responsibilities

- Implementing the agreed security products and practices from this policy
- Recommending new security measures as they become available.

School Responsibilities

- The failure of any none recommended security products and procedures.
- Any staff training required to help keep the school data and network safe.

Policy Review

hi-impact will review this policy on an annual basis, and it will be updated with any products or services that will provide enhanced security products and practices.

Schools will be advised of new products and services as they become available.

In the meantime, if you have any questions, suggestions or feedback, please contact Jamie Gray, at jamiegray@hi-impact.co.uk.

1. Antivirus Policy

All school devices running Windows and MacOS operating systems will be covered by adequate antivirus protection.

An adequate antivirus solution is critical, and one of the first lines of defence to prevent intrusions into your network. Hi-impact has developed a partnership with Watchguard, who are world-leading providers for network security products. Their solution, Panda Adaptive Defence 360 (AD360) is a next generation antivirus, and as such, our recommended product.

Panda Adaptive Defence 360 includes a Zero-Trust Application Service that allows for continuous monitoring of devices where it is installed, collecting and analysing all activity. From there, it reveals suspicious behaviours of users, machines, and background processes on machines within the network, with features that block such offending processes. In addition, the Threat Hunting Service discovers new vulnerabilities and methods that attackers use to conceal their methods. These two features are included in their advanced endpoint agent, and work together to detect and classify 100% of the activity on all machines on the network.

If purchased, Hi-impact will ensure that AD360 is deployed to all school computers. Should a school opt to supply their own antivirus protection, Hi-impact's technical staff will state whether this solution meets their definition of 'adequate'. In the event of the solution in question not meeting this standard, technical staff will ensure all devices are covered by the solution in question, but will not accept responsibility for any breaches that occur as a result.

As Chromebooks have a built-in antivirus solution, they do not require a third-party solution to be installed on them.

All St George's Windows devices are protected with AD360.

2. Patch Management Policy

All IT systems owned and operated by the school must be licensed appropriately, in addition to running up-to-date patches of operating systems and application software. In order to ensure that a school's IT systems are protected from known vulnerabilities, security patches will be deployed in a suitable time frame. Unless prevented by known issues, patches should be deployed according to the following schedule:

Classification of Patch	Full Deployment Within
Critical	14 days
High	14 days
Medium	21 days
Low	28 days

Hi-impact technical staff will ensure that a patch management system for Windows Updates is deployed to all Windows Devices through our Remote Management Solution (Datto RMM). Technicians will ensure that this system is updated and maintained regularly with new updates and patches, monitoring its effectiveness across all devices.

On Apple devices, updates for MacOS, iPadOS, and iOS, in addition to updates to applications, will be set to install automatically. Likewise, ChromeOS updates will be set to install automatically. Technicians will monitor that updates are installed.

All new IT systems will be updated and patched before being used in school, to avoid the introduction of any vulnerabilities to the network.

An IT system or application that is retired by its manufacturer will be reported to the school via the annual IT Audit, where recommendations will be made for alternatives for that device or software. Should the school decide to continue running a device or application that has been advised as end-of-life, this will be the Schools' sole responsibility should issues arise.

3. Backup Policy

Prevention is a crucial first step in security, but breaches do occur even with the most stringent protection in place. For those rare occasions, having a multi-layered backup policy is vital. Hi-impact technical staff have spent many years working with various solutions and strategies in place, and will recommend a series of onsite and offsite backup measures to give you as much chance as possible of recovering data, should a loss, corruption, or deletion of that data occur.

Hi-impact recommends the 3-2-1 backup structure with the offline rule as advised by the National Cyber Security Centre (NCSC). The 3-2-1 structure means that you have at least 3 copies of the data, on 2 different devices, and 1 must be offsite. The offline rule means that one of your on-site backups must be disconnected from the network once the backup is completed. The below backup mediums are recommended to meet these requirements and provide the best protection of data.

External Backups:
An external backup is the best form of recovery following a site-wide disaster such as a flood or fire and is the backup that meets the Offline Rule.The school should have two external hard drives with a capacity of at least double the storage capacity of the main school server. One drive will be connected to the server and the other stored in a fireproof safe away from the server at any given time. A full server backup of the main school server will be completed to the connected hard drive each night. The drives will be swapped during the school’s scheduled Tech Visit by hi-impact Technical Staff to ensure there is always a recent backup in the school’s fire proof safe.

St George’s has two 8TB external hard drives that are swapped during the Tech Visit on Wednesdays.

Internal Network Backups:
The school should have a network storage device dedicated to saving backups of all school servers. This could be a large hard drive in a server or a Network Accessible Storage (NAS). A full server backup of all servers will be scheduled to run every night to this backup location. This is known as a System Image Backup, which acts as a snapshot of the server at the moment of the backup. This is the quickest method of recovery after a disaster.

St George’s has a nightly backup of all servers to a dedicated backup server located in the Switch Cabinet in the Lower Site Staff Room.

Cloud Backups:
A cloud backup solution should be in place to backup the SIMS Database and the most important Admin Data every night. This means that a copy of the most important data is held off-site and separate from the school system. Hi-impact strongly recommends using Redstor as the school’s cloud backup solution.

All Redstor data is held on servers within the UK. This backup contributes to the offsite requirement of the 3-2-1 model.

St George's has 100GB from Redstor which backs up the SIMS FMS database, Papercut Printer Management database, Paxton NET2 Door Controller database, SMT Shared Area and the SMT & Admin User Areas.

SAAS Protection:
To aid with remote working following the COVID-19 pandemic, the school may have migrated their Shared and individual User Areas to Google Drive. As secure and reliable as Google is, it does not have a complete backup built in and so a third-party solution is required which is called SAAS Protection. Hi-impact strongly recommends Datto SAAS Protection as a trusted third-party solution. All Datto data is held on servers within the UK. Datto completes a backup every hour and data can be restored through the Datto Portal. This backup contributes to the offsite requirement of the 3-2-1 model.

St George's protects 10 users and all of the Google Shared Drives with Datto SAAS Protection.

Shadow Copies:
Shadow copies allow for the instant restoration of previous versions of data, in the event of that data's deletion or accidental amendment by users. This system will create a copy of each data drive on the server at 07:00 and 12:00, and these copies will be stored for 30 days. This is a built-in feature of Windows and will be enabled by default by hi-impact.

Backups **do not guarantee 100% protection against data loss.** Multiple factors can have an effect on the success of a restoration, including, but not limited to the date/time of the breach, or the severity of the attack.

4. Password Policy

Password-related breaches can be caused by human carelessness, brute force attacks, systematic computerised hacks or simply neglect. There are numerous measures that can be put in place to minimise such risks and hi-impact have a set of recommended guidelines that your school should adopt:

- Passwords must offer an adequate level of security to protect systems and data.
- Multi-factor authentication should be enabled on as many logins to cloud apps as possible, especially accounts that may hold a greater amount of confidential information (e.g. Headteacher, SENDCo & Business Manager email accounts). This provides an additional layer of security for these accounts.
- All school staff passwords should meet the minimum complexity requirements:
    - Password length of at least 12 characters,
    - Contain three random words alongside numbers and symbols,
    - Doesn't contain any easily guessable information (e.g. users first name or job title).
    - Follow best-practice guidelines for password security.
- All school staff passwords should be unique and not be reused.
- Passwords should never be written down or saved in an insecure location (e.g. Word Documents, Post-it notes, notebooks, etc.).
- School Staff are advised to use password vaults and password generators (such as LastPass) to assist in creating secure passwords and to securely store them. Where a password vault is used, it must itself be protected by a strong password and multi-factor authentication.
- All passwords should be changed immediately if they have been compromised – or suspected to have been compromised.

Hi-impact will run password checks once a year and force any user with a common or compromised password to update their password to comply with the above policy. Hi-impact further protect user accounts by locking them if more than ten incorrect password attempts are entered within a five minute time period. The account will remain locked until the staff member contacts Hi-impact via a Tech Ticket to confirm it was them attempting to log in and then the account will be unlocked.

Although it is not recommended, the school may opt to modify this password policy. hi-impact will not accept any responsibility for any breach that may occur as a result of the Schools' decision to vary the password policy. For password policies fully in compliance with the above recommendations, hi-impact will be responsible for ensuring that the policies are active and functioning.

Password policies DO NOT guarantee 100% protection against a breach, but are an essential protection against them.

All users will be issued a uniquely named user account. Newly created accounts and password resets organised by hi-impact Technical Staff will have a randomly generated password and the user will be required to create a new password at next login. Generic user accounts that are used by more than one person shall not be used by staff.

Where schools have their own in-house technicians or staff who are administrators to key systems, it is the school’s responsibility to ensure these users have passwords that are highly complex and unique. It is recommended that these users do not use their administrator accounts on a day to day basis but have a separate account with standard user permissions.

5. Data Security Policy

Data is valuable and in many cases extremely confidential and sensitive. Taking precautions to minimise the risk of losing data or allowing it to fall into the wrong hands is vital.

Mobile Devices (Mobile Phones, iPads & Tablets):
All mobile devices, including staff’s personal devices, should be protected by a unique passcode. On school devices, this will be managed through the administration of the device itself. Staff will be required to enter a passcode into the device when they use it for the first time. This passcode should only be shared among school staff. School mobile devices should only be used for school activities by authorised staff members. Mobile devices should be set to auto-lock after a maximum of five minutes of inactivity, again this will be managed through the administration of the device.

Staff Laptops:
Staff should not use their own laptops or personal computers to store school data with Personally Identifiable Information (PII). School data that is held on staff laptops should only be in the “User Area” and is accessible outside of schools via Offline Files. The offline files cache will be encrypted through an administrative policy on the school server.

Google Drive:
To aid with remote working following the COVID-19 pandemic, the school may have migrated their Shared and individual User Areas to Google Drive. School Google Drive data should only be accessed on school devices or online through Google Docs on a personal device. School Google Drive data should never be downloaded to personal devices. Google will automatically monitor the activity of users and block any suspicious login attempts. School Google Accounts should be set to auto-logout after a maximum of eight hours of inactivity, this can be enforced through the school’s Google Administrative Settings.

Device Auto-Locking:
Any device that leaves the school site, or is used by Office Staff or SMT, should have an auto-lock policy enabled, this will be turned on by default by hi-impact. The recommended lockout time is 10 minutes for non-teaching devices and 30 minutes for teaching devices. It is recommended that staff manually lock their device each time when moving away from the screen.

Staff Training:
Hi-impact strongly recommends that all staff attend basic Cyber-Security training to ensure they are fully aware of why such robust policies are required to keep data safe from the risks of cyber attacks. Staff should be fully aware of their responsibilities when managing and transporting data.

Measures put in place by hi-impact technical staff to protect against data loss can be undermined if data is not stored and transported in the recommended way.

6. Internet Security & Filtering Policy

As more and more systems move to the cloud, keeping the school community safe online, and protecting the internal network from risks, has never been more important. At the very minimum a school is required to have a filtering system that will protect children from inappropriate content, and a firewall that will prevent unauthorised access to the network.

Hi-impact strongly recommends EXA Quantum to filter the school's internet connection. This filtering is automatically applied for schools with the hi-impact Internet Service Level Agreement (SLA). This system provides key word, URL and category filtering to all internet traffic and has been designed specifically for schools. EXA constantly updates their keyword and website block lists and, by default, hi-impact will apply their rules. Should a website need to be blocked or unblocked, a helpdesk ticket must be submitted to hi-impact and the website will be assessed by technical staff. If a blocked site is found to have been blocked unnecessarily then it will be unblocked. If the unblock request is for a website that has been blocked for a substantive reason then the request will be placed on hold and the headteacher will be required to submit the request in writing to unblock the website. The request can be sent to support@hi-impact.co.uk.

If the school has the Hi-impact Internet SLA, hi-impact will install and manage the school's firewall. External access to the school's network will only be achievable through the three following routes:

- Remote access from the Hi-impact Office.
- Remote access from the Wirral Software Support Team Office for SIMS Support and Bursar access.
- VPN from a school device while a staff member is working at home.

Access from all other locations will be denied by the firewall.

St George's uses EXA Quantum to filter it's internet content and the firewall is managed by hi-impact.

7. Remote Access Policy

Any external access to the school network is a potential risk so managing that risk effectively is essential. Hi-impact strongly recommends that remote access to the network be limited to the fewest staff possible and only be installed on school-owned and managed computers. For example, if a school uses Google Drive to host their Shared Drives, the only users that will require remote access are the people that require SIMS or FMS at home.

To facilitate remote access to the school network in the most secure way, Hi-impact will set up a Virtual Private Network (VPN) connection on each computer that will be used at home. A VPN creates a secure tunnel through the internet between the computer and the school network and is authenticated by either a pre-installed certificate which is renewed every 12 months, or by entering a code that, combined with an installed secret key, generates a login to the VPN that is unique to that instance.

Currently at St George's, remote access is limited to John Evans and Sarah Jones using the Fortigate VPN Client.

8. Email Policy

The School's e-mail facility is intended to promote effective communication between staff and external providers on matters relating to the School's activities, and access to the School's e-mail facility is provided for work purposes only.

Hi-impact will enable all the recommended spam and phishing controls as recommended by the email provider (Office 365 or Google Workspace) and will monitor any alerts that come through from the email client regarding unusual activity.
Hi-impact strongly recommends implementing the following precautions on school emails:

- Staff should not use personal email accounts for school use.
- Staff should remember to log out of their email accounts when they are finished using them.

It is strongly recommended that all staff participate in basic Cyber-Security training to be able to recognise a malicious email and know the appropriate actions to take. All staff should double-check the sender email address, subject and body of the email before opening any attachments. Hi-impact will not accept any responsibility for any virus or other risk introduced to the network following a staff member opening a malicious email.

9. VOIP Data Policy

Many schools now have an advanced phone system with the ability to save voicemail and phone call recordings.

Only authorised school staff members and hi-impact staff members will have access to the school's phone portal. Hi-impact staff are not permitted to access any recordings from the school phone system due to GDPR. We will only provide guidance for school staff to gain access to the recordings.

10. Server Configuration Policy

The school servers are not something school staff are likely to have any contact with but are the most essential parts of the school network. Due to the importance of the servers, Hi-impact recommends the following:

- Servers should be physically located in a lockable, secure room that can only be accessed by support staff, or inside a locked cabinet that prevents interference or theft.
- Only hi-impact staff should be able to log into a server. If a school has on-site Technical Support then access will be provided as long as their accounts' meet all complexity requirements. The school will be responsible for any security breaches that occur as a result of an on-site administrator account being compromised.
- All data stored on the servers is secured by appropriate permissions and end-user access is dependant on security group membership.
- Settings on school computers are governed by Group Policies developed by Hi-impact. Any new settings will be configured and deployed by hi-impact as they become available.

11. WiFi Security Policy

Wireless networks are essential to the smooth operation of a modern school. The range of the school wireless network is mostly confined to the school premises, which helps contain the likelihood of a breach through WiFi access. It is strongly recommended that all Wireless Access Points connected to the network are registered and approved by Hi-impact.

A strong WiFi connection password should be set for the WiFi, and only made available to authorised users. The connection password should not be written down nor left in an easily accessible location. These measures will help to prevent unknown devices from connecting to the network, and the network becoming vulnerable. Should the connection password need to be changed, please note that this is neither a quick nor straightforward endeavour, and it will cause disruption to the school's network and therefore to the work of the school whilst it is being implemented.

The school WiFi network should not be used to provide wireless access for visitors, and a Guest WiFi network can be set up if needed. The Guest WiFi is a more restricted connection which only allows access to the internet, and does not allow connection to any other device on the school network. This limits the amount of devices connecting to the school network and creating potential routes of vulnerability.

12. Staff Leavers Policy

When a member of staff ceases employment with the school, access to school information and systems will need to be revoked. Hi-impact will take the appropriate measures to disable their local user accounts, as well as disabling their school email account, and forwarding email traffic to another staff member if required. It is the school's responsibility to inform hi-impact of the departure of a staff member, in order for appropriate revocation of network access and other actions to be initiated.

If any staff members ceases employment with Hi-impact, Hi-impact's will to inform the school of their departure, as well as revoking access to Hi-impact systems and any remote access to school systems. It is recommended that the School DBS list is updated to ensure that a former hi-impact employee is not accidentally granted access to school systems.

13. Bring Your Own Device (BYOD) Policy

This policy is intended to protect the security of the School's data, and its overall network. Staff are permitted to bring personal mobile devices (mobile phones) onto the school premises, but the following recommendations should be followed:

- Staff should not use their own devices to store school data that contains Personally Identifiable Information
- All mobile devices that leave the school premises (Mobile phones, iPads, Laptops, etc.) should be protected by a passcode, password, or PIN.
- Hi-impact strongly recommends that portable USB storage devices (including USB "pen drives" and portable Hard Drives) are not used, they pose a potential security risk in the event that they are lost and contain sensitive data. Hi-impact are able to apply a policy on the school server(s) to block the use of such devices in agreement with the school.
- Any personal device that a staff member would like to use in school must be checked and approved by Hi-impact to ensure it meets minimum security standards and is running the required apps. The device must have the latest security patches installed, have up-to-date anti-virus software and be protected by a password, PIN or biometrics. Staff should not connect a new device to the network without consulting Hi-impact; the device could pose a potential risk by carrying a virus.

14. 3rd Party Providers

Hi-impact systems in schools are complex, and not all third party providers' systems work as intended if they are installed incorrectly, and in some cases, cannot be installed at all. Hi-impact recommends that if any third party software or installations are needed on the school network, that Hi-impact are consulted first, as they can give recommendations, or even recommend alternative solutions that may be more beneficial.

In the event that changes are made to a school network or systems without consultation with Hi-impact, and there is an adverse effect on the network or system's operation, Hi-impact will not be responsible for any issues that arise as a result. The school will be liable for any costs incurred to resolve the aforementioned issues.

15. Data Disaster Recovery Policy

One of the most important considerations to be made in regards to security is the response to a disaster, as even with the most stringent policies in place, disasters can occur. Plans to minimise the impact of a breach, and recovering lost data and operational ability can make the difference between hours or weeks of inoperability. Planning for a worst-case scenario can also ensure that any downtime of the school's network, and time taken for the retrieval of lost data, can be kept to a minimum.

The Disaster Recovery Policy has been developed by Hi-impact to inform schools of the effective and efficient support that can be provided.

What is a Disaster?

In this policy a Disaster is defined as loss of or damage to part, or all, of the school's ICT infrastructure, which would have a high, or very high, negative business and educational impact upon the school.

This includes:

a) Total loss of one site (i.e. due to fire damage)

b) Loss or technical failure of one or more network servers

c) Loss or technical failure of network infrastructure i.e. hub/switch/router/comms link

d) Major attack on the system by a virus or other type of malware.

The following policy highlights what systems your school currently has in place and what systems are available to increase the security and safety of the schools' data. Systems that are 'greyed out' are not currently in place and may require further discussion between Hi-impact and the school.

Maintenance and Updates:

Servers and workstations are routinely checked for software and hardware faults. Antivirus definitions and Microsoft Updates are kept up to date.

Redundancy:

Server hard drives are configured with a minimum of RAID 1 redundancy, ideally RAID 10. This means the server can withstand a failed hard drive without any data loss.

Shadow Copies:

All data stored on the servers is copied twice a day (8:00 and 12:00) using a Microsoft system called Shadow Copies. All users are able to retrieve deleted work from anywhere on the network with a right click of the mouse.

Cloud Backup:

The Admin data and the SIMS server are backed up nightly using an online cloud backup solution. This means that all the schools' Admin data is offsite and up to date. Hi-impact uses a system called Redstor, which is one of the market leaders in this field, and the only service to be authorised by Capita. All data is held within the UK, thus meeting UK GDPR requirements.

Internal Backup:

A full server backup is scheduled to run every night to an internal drive within a backup server or a NAS. This is a system image backup, and is the quickest way to restore the server in the event of a catastrophic failure.

External Backup:

The servers are fully backed up to two external hard drives which are rotated on a weekly basis. One drive should always be kept in a fireproof safe within the school, situated away from the server. This is in case of a site-wide disaster such as a flood or fire.

Power:

The server is powered through a Uninterruptible Power Supply (UPS) to prevent damage in the event of a power cut or power surge. In the event of a power cut, its function is to keep the server powered up long enough for it to shut down safely.

Email & Google Drive:

Email is cloud based and therefore accessible as long as there is an Internet connection. In the event of prolonged loss of Internet connectivity then an alternative connection could be established using a 3G device such as a phone or dongle.

SAAS Protection:

Key Google or Microsoft accounts are backed up to a third-party backup solution. This solution will backup all email, drives (including Shared Drives), contacts and calendar data for the protected users. It is essential that the super admin for the school system is one of the protected accounts to ensure all Shared Drives are protected. SAAS Protection allows us to restore data to Google Workspace and Microsoft 365 in the case of a disaster.