Saint GREGORY'S
Bath

Security Breach Prevention and Management Policy

Title	Security Breach Prevention and Management Policy	
Prepared By	Stuart Hodder - Network Manager	December 2019
Checked By	Karen Tyler - Data Manager	December 2019
Last Approved By	Governors Finance and Premises Committee	September 2022
Version	V01.01	
Document Update	September 2023	

Version	Date	Amendments
V01.00	February 2020	Approved by Governors
V01.01	September 2022	Staff roles updated

Contents:

Statement of intent

St Gregory’s is committed to maintaining the confidentiality of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible by the appropriate individuals. It is therefore important to uphold high standards of security, take suitable precautions and to have systems and procedures in place that support this.

The school recognises, however, that breaches in security can occur, particularly as the majority of information is stored online or on electronic devices which are increasingly vulnerable to cyber-attacks. This being the case, it is necessary to have a contingency plan containing procedures to minimise the potential negative impacts of any security breach, to alert the relevant authorities and to take steps to help prevent a repeat occurrence.

The following members of staff are responsible for insuring school data is kept secure and conforms to the current GDPR and Data Protection Act.

Roles and Responsibilities

Ann Cusack - Headteacher and Data Controller
Shelley Tuke - Designated Safeguarding Lead
Gerry Cross – Facilities and ICT Manager
Stuart Hodder - Network Manager
Karen Tyler - Data Manager and Data Protection Officer
Adrian Foley – Head of ICT

Contact Details

Headteacher or Acting Head - Ext 203
cusacka@st-gregorys.org.uk

Designated Safeguarding Lead – Ext 295
tukes@st-gregorys.org.uk

Network Manager and IT Support - Ext 224
hodders@st-gregorys.org.uk

Data Manager and Data Protection Officer – Ext 282
tylerk@st-gregorys.org.uk

Facilities and ICT Manager – Ext 287
crossg@st-gregorys.org.uk

Head of ICT
foleya@st-gregorys.org.uk

1. Legal framework

1.1 This policy has due regard to statutory legislation and regulations including, but not limited to, the following:

- The Data Protection Act 2018
- The Computer Misuse Act 1990
- The General Data Protection Regulation (GDPR)

1.2 This policy has due regard to the school's policies and procedures including, but not limited to, the following:

- Online Safety and Social Media Policy
- Data Protection Policy
- IT Acceptable Use Policies (Students, Staff)

2. Types of security breach and causes

2.1 **Unauthorised use without damage to data** – involves unauthorised persons accessing data on the school system, e.g. 'hackers', who may read the data or copy it, but who do not actually damage the data in terms of altering or deleting it.

2.2 **Unauthorised removal of data** – involves an authorised person accessing data who removes the data to pass it on to another person who is not authorised to view it, e.g. a staff member with authorised access who passes the data on to a friend without authorised access – this is also known as data theft. The data may be forwarded or deleted altogether.

2.3 **Damage to physical systems** – involves damage to the hardware in the school's ICT system which may result in data being inaccessible to the school and/or becoming accessible to unauthorised persons.

2.4 **Unauthorised damage to data** – involves an unauthorised person causing damage to data either by altering or deleting it. Data may also be damaged by a virus attack rather than a specific individual.

2.5 Breaches in security may be caused as a result of actions by individuals which may be accidental, malicious or the result of negligence. These can include:

- Accidental breaches, e.g. as a result of insufficient training for staff so they are unaware of the procedures to follow.
- Malicious breaches, e.g. as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.
- Negligence, e.g. as a result of an employee that is aware of school policies and procedures, but disregards these.

2.6 Breaches in security may also be caused as a result of system issues which could involve incorrect installation, configuration problems or an operational error. These can include:

- Incorrect installation of anti-virus software and/or use of software which is not the most up-to-date version, meaning the school software is more vulnerable to a virus.
- Incorrect firewall settings are applied, e.g. access to the school network meaning individuals other than those required could access the system.
- Confusion between backup copies of data, meaning the most recent data could be overwritten.

3 Roles and responsibilities

3.1 The Headteacher is responsible for implementing effective strategies for the management of risks posed by internet use and to keep its network services, data and users secure.

3.2 The Network Manager and the Data Protection Officer are responsible for the overall monitoring and management of data security.

3.3 The Network Manager and the Data Protection Officer are responsible for establishing a procedure for managing and logging incidents. They will report to the Headteacher.

3.4 The Governing Body is responsible for holding regular meetings with the Headteacher and the Data Protection Officer to discuss the effectiveness of data security and to review incident logs.

3.5 All members of staff and students are responsible for adhering to the processes outlined in this policy alongside the school's Online Safety and Social Media Policy.

4 Secure configuration

4.1 An inventory will be kept of all IT hardware and software currently in use at the school, including mobile phones and other personal devices provided by the school. This will be stored in the EVERY Online Assets system and will be audited three times per year and ongoing live adjustments ensure it is up-to-date.

4.2 Any changes to the IT hardware or software will be documented using the inventory, and will be authorised by the Network Manager before use.

4.3 All systems will be audited three times per year to ensure the software is up-to-date. Any new versions of software or new security patches will be added to systems, ensuring that they do not affect network security, and will be recorded on the inventory.

4.4 Any software that is out-of-date or reaches its 'end of life' will be removed from systems, i.e. when suppliers end their support for outdated products such that any security issues will not be rectified.

4.5 All hardware, software and operating systems will require passwords for individual users before use. Passwords will be changed every 90 days based on group policy settings on the servers to prevent access to facilities which could compromise network security.

4.6 The school believes that locking down hardware, such as through the use of strong passwords, is an effective way to prevent access to facilities by unauthorised users and recommend all staff and students use strong passwords. Strong passwords are currently enforced due to operational issues.

5 Network security

5.1 The school will employ firewalls, web content filters and malware protection in order to prevent unauthorised access to the systems.

5.2 As the school's firewall is managed internally by the Network Manager, the firewall management service will be thoroughly investigated by the Network Manager to ensure that:

- Only the Network Manager has permissions to access the firewall admin portal to manage the firewall rules or content filter modifications.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.
- Any compromise of security through the firewall will be recorded using an incident log and reported to the Headteacher, the Data/GDPR Lead, and the IT Lead for SLT. The Network Manager will react to any security threats to find new ways of managing the firewall and seek help from our paid support professionals if needed.

6 Malware prevention

6.1 The school understands that malware can be damaging for network security and may enter the network through a variety of means, such as email attachments, social media, malicious websites or removable media controls.

6.2 The Network Manager will ensure that all school devices have secure malware protection and undergo regular malware scans. We employ antivirus with Malware, Ransomware and Web and email protection on all devices.

6.3 The Network Manager will ensure that our antivirus software updates and virus definitions are applied to all devices.

6.4 Filtering of websites, as detailed in section 7 of this policy, will ensure that access to websites with known malware is blocked immediately and reported to the Network Manager.

6.5 The school uses mail security technology, which will detect and block any malware that is transmitted by email. This will also detect any spam or other messages which are designed to exploit users.

6.6 The Network Manager will review the mail security technology on a termly basis to ensure it is kept up-to-date and effective.

7 User privileges

7.1 The school understands that controlling what users have access to is important for promoting network security and safeguarding. User privileges will be differentiated, i.e. students will have different access to data and the network than members of staff.

7.2 The Data Protection Officer will investigate what users need to have access to and will communicate this to the Network Manager, ensuring that a written record is kept.

7.3 The Network Manager will ensure that user accounts are set up to allow users access to the facilities required, in line with the Data Protection Officer's instructions, whilst minimising the potential for deliberate or accidental attacks on the network. The Data Manager will ensure that SIMS is set up so that users can access only the data they need to be able to see.

7.4 The Network Manager will ensure that websites are filtered on a weekly basis for inappropriate and malicious content. Any member of staff or student that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 12 of this policy.

7.5 All users will be required to change their passwords every 90 days and should use upper and lowercase letters, as well as numbers, and special characters to ensure that passwords are strong as a recommendation. Complex password enforcement is enabled via group policy. Users will also be required to change their password if they become known to other individuals.

7.6 Students are responsible for remembering their passwords, however, the Network Manager and teaching staff will be able to reset them if necessary.

7.7 The 'master administrator' password used by the Network Manager will be made available to the Headteacher or any other nominated senior leader and will be kept in the school office or safe as part of the schools Recovery Policy.

7.8 A multi-user account will be created for visitors to the school, such as Supply Teachers, and access will be filtered as per the Data Protection Officer's instructions. Usernames and passwords for this account will be changed on a yearly basis and will be provided as required.

7.9 We employ an automated user provisioning system that automatically deletes inactive users or users who have left the school. The Network Manager will manage this provision to ensure that all users that should be deleted are and that they do not have access to the system. The system was configured and is managed by the solution provider. The Network Manager will review the system on a termly basis to ensure the system is working as expected.

8 Monitoring usage

8.1 Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by students or staff.

8.2 The school will inform all students and staff that their usage will be monitored, in accordance with the school's IT Acceptable Use Policy and Online Safety and Social Media Policy.

8.3 If a user accesses inappropriate content or a threat is detected an alert will be sent to the Network Manager via Impero. The Network Manager will monitor Impero on a daily basis and report any configuration recommendations to the Facilities and ICT Manager.

8.4 Alerts will identify the user, the activity that prompted the alert and the information or service the user was attempting to access.

8.5 The Network Manager and the Data Protection Officer will record any critical alerts using an incident log and will report this to the Headteacher and IT Lead for SLT. All incidents will be responded to in accordance with section 12 of this policy and as outlined in the Online Safety and Social Media Policy.

8.6 All data gathered for investigation and monitoring usage will be kept in a filing cabinet in the IT Office or passed on to the Facilities and ICT Manager for easy access when required. This data may be used as a method of evidence for supporting a not yet discovered breach of network security. In addition, the data may be used to ensure the school is protected and all software is up-to-date.

9 Removable media controls and home working

9.1 The school understands that students and staff may need to access the school network from areas other than on the premises. Effective security management will be established to prevent access to or leakage of data as well as any possible risk of malware.

9.2 The Network Manager will ensure all school devices are password protected and locked down by security permissions and will ensure windows updates and anti-virus updates are automatically applied.

9.3 **USB drives**

The Network Manager and the Data Protection Officer explicitly state that no students or staff personal data is to be kept on any portable device or home device as it could get lost, stolen or allow personal data to get into the wrong hands.

Staff should refrain from using their personal storage devices where the school provides alternatives, such as staff laptops and tablets. They should, where possible, make use of Microsoft One Drive access via Office 365 or via Remote Access to keep data secure and not download personal data on to home devices.

St Gregory’s currently employ a ‘No USB’ enforcement via group policy on the school machines, unless explicitly agreed by the Network Manager who will ensure all security measures are in place to minimise any threat to the school and its systems if permission is granted.

9.4 If students and staff are instructed that they are able to use their personal devices they will ensure that they have an appropriate level of security and firewall to prevent any compromise of the school’s network security. This will be checked by the Network Manager.

9.5 When using laptops, tablets and other portable devices, the Network Manager will determine the limitations for access to the network, as described in section 5 of this policy.

9.6 Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether it be on or off school premises.

9.7 All data will be held on systems centrally in order to reduce the need for the creation of multiple copies and/or the need to transfer data using removable media controls.

9.8 The Wi-Fi network at the school is password protected by a radius server (uses internal user credentials for security). Staff and students are only allowed to use the SGCC_BYOD with their personal devices, such as mobile phones or tablets.

9.9 SGCC_Staff is only used for internal school devices and added under the instruction of the Network Manager.

10 Backing-up data

10.1 We use a fully managed backup solution that is connected to the provider's onsite backup appliance which replicates to a secure datacentre in the cloud.

10.2 The backup providers perform automated incremental backups nightly on the basis of any data that has changed since the previous back-up. If we need to restore or backup any data we call the provider's support team.

10.3 All backups are password protected and encrypted with a secure VPN connection to the remote data centre.

10.4 The data centre is fully GDPR compliant and recommended for disaster and ransomware recovery.

10.5 The providers are the only people that can access our data from the secure data centre.

11 User training and awareness

11.1 The Head of ICT and the Headteacher/SLT will arrange training for students and staff when new intake year or new staff members join to ensure they are aware of how to use the network appropriately in accordance with the IT Acceptable Use Policy and the Online Safety and Social Media Policy.

11.2 Training for all staff members will be arranged by the IT Lead for SLT/Network Manager and the Data Protection Officer at the discretion of the Headteacher following an attack or significant update.

11.3 Through training, all students and staff will be aware of who they should inform first in the event that they suspect a security breach and who they should inform if they suspect someone else is using their passwords.

11.4 All staff will receive training as part of their induction programme as well as any new staff that join the school.

11.5 All users will be made aware of the disciplinary procedures for the misuse of the network leading to malicious attacks, in accordance with the process detailed in the Online Safety and Social Media Policy.

12 Security breach incidents

12.1 Any individual that discovers a security data breach will report this immediately to the Headteacher, the Network Manager and the Data Protection Officer.

12.2 When an incident is raised the Network Manager and the Data Protection Officer will record the following information:

- Name of the individual who has raised the incident
- Description of the incident
- Description of any perceived impact
- Description and identification codes of any devices involved, e.g. school-owned laptop
- Location of the equipment involved
- Contact details for the individual who discovered the incident

12.3 The school's Network Manager and the Data Protection Officer will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

12.4 The Data Manager and the Network Manager, as quickly as reasonably possible, will ascertain the severity of the breach and determine if any personal data is involved or compromised.

12.5 The Data Manager and the Network Manager will oversee a full investigation and produce a comprehensive report.

12.6 The cause of the breach and whether or not it has been contained will be identified, ensuring that the possibility of further loss/jeopardising of data is eliminated or restricted as much as possible.

12.7 If the Data Manager and the Network Manager determine that the severity of the security breach is low, the incident will be managed in accordance with the Data Breach Procedure and Response Plan.

- In the event of an internal breach the incident is recorded using an incident log and by identifying the user and the website, network drive or service they were trying to access.
- The Headteacher will issue disciplinary sanctions to the student or member of staff in accordance with the processes outlined in the Online Safety and Social Media Policy or the Acceptable Use Policy.
- The Network Manager will work with the third-party firewall provider to provide an appropriate response to the attack, including any in-house or external firewall rules.

12.8 Any further action which could be taken to recover lost or damaged data will be identified. This includes the physical recovery of data as well as the use of back-ups.

12.9 Where the security risk is high the school will establish what steps need to be taken to prevent further data loss which will require support from various school departments and staff. This action will include:

- Informing relevant staff of their roles and responsibilities in areas of the containment process.
- Taking systems offline.
- Retrieving any lost, stolen or otherwise unaccounted for data.
- Restricting access to systems entirely or to a small group.
- Backing up all existing data and storing it in a safe location.
- Reviewing basic security, including:
  - Changing passwords and login details on electronic equipment.
  - Ensuring access to places where electronic or hard data is kept is monitored and requires authorisation.

12.10 Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Headteacher will inform the Police of the security breach.

12.11 The Network Manager will test all systems to ensure they are functioning normally, and the incident will only be deemed 'resolved' when it has been assured that the school's systems are safe to use.

13 Assessment of risks

13.1 The following questions will be considered by the Data Manager and the Network Manager in order to fully and effectively assess the risks that the security breach has brought, and to help take the next appropriate steps. All relevant questions will be clearly and fully answered in the Data Manager and the Network Manager's reports which will record:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the Data Protection Act 2018; some data is sensitive because of its very personal nature (e.g. health records) while other data types are sensitive because of what might happen if it is misused (e.g. bank account details).
- Is it possible to identify what has happened to the data – has it been lost, stolen, deleted or tampered with?
- If the data has been lost or stolen, were there any protective measures in place to prevent this, such as data and device encryption?

- If the data has been compromised, have there been effective measures in place that have mitigated the impact of this, such as the creation of back-up tapes and spare copies?
- Has individuals' personal data been compromised – how many individuals are affected?
- Who are these individuals – are they students, staff, governors, volunteers, stakeholders, suppliers?
- Could their information be misused or manipulated in any way?
- Could harm come to individuals? This could include risks to the following:
    - Physical safety
    - Emotional wellbeing
    - Reputation
    - Finances
    - Identity
    - Private affairs becoming public
- Are there further implications beyond the risks to individuals? Is there a risk of loss of public confidence/damage to the school's reputation or risk to the school's operations?
- Who could help or advise the school on the breach? Could the LA, external partners, authorities, or others provide effective support?

13.2 In the event that the Network Manager and Headteacher, or other persons involved in assessing the risks to the school, are not confident in the risk assessment they will seek advice from the Information Commissioner's Office (ICO).

14 Consideration of further notification

14.1 The school will consider whether there are any legal, contractual or regulatory requirements to notify individuals or organisations that may be affected or who will have an interest in security (see 14.8 onwards for specific GDPR requirements about personal data).

14.2 The school will assess whether notification could help the individual(s) affected and whether individuals could act on the information provided to mitigate risks, e.g. by cancelling a credit card or changing a password.

14.3 If a large number of people are affected or there are very serious consequences the ICO will be informed.

14.4 The school will consider who to notify, what to tell them and how they will communicate the message, which may include:

- A description of how and when the breach occurred and what data was involved. Details of what has already been done to respond to the risks posed by the breach will be included.
- Specific and clear advice on the steps they can take to protect themselves, and what the school is willing to do to help them.

- A way in which they can contact the school for further information or to ask questions about what has occurred.

14.5 The school will consult the ICO for guidance on when and how to notify them about breaches.

14.6 The school will consider, as necessary, the need to notify any third parties – Police, insurers, professional bodies, funders, trade unions, website/system owners, banks/credit card companies – who can assist in helping or mitigating the impact on individuals.

Under the GDPR, the following steps will be taken if a breach of personal data occurs:

14.7 The school will notify the ICO within 72 hours of a breach where it is likely to result in a risk to the rights and freedoms of individuals.

14.8 Where a breach is likely to result in significant risk to the rights and freedoms of individuals, the school will notify those concerned directly with the breach.

14.9 Where the breach compromises personal information, the notification will contain:

- The nature of the personal data breach including, where possible:
  - The type(s), e.g. staff, students or governors, and approximate number of individuals concerned.
  - The type(s) and approximate number of personal data records concerned.
- The name and contact details of the Data Manager and the Network Manager or other person(s) responsible for handling the school's information.
- A description of the likely consequences of the personal data breach.
- A description of the measures taken, or proposed, to deal with and contain the breach and, where appropriate, of the measures taken to mitigate any possible adverse effects.

15 Evaluation and response

15.1 The Network Manager will establish the root of the breach and where any present or future risks lie.

15.2 The Data Protection Officer will consider the data and contexts involved.

15.3 The Network Manager and the Headteacher will identify any weak points in existing security measures and procedures. The GDPR lead and IT Lead for SLT will also be consulted

15.4 The Data Manager, the Network Manager and the Headteacher will identify any weak points in levels of security awareness and training.

15.5 The Data Manager and the Network Manager will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

16 Monitoring and review

16.1 This policy will be reviewed by the Headteacher, in conjunction with the Data Protection Officer and the Network Manager, on an annual basis.

16.2 The Data Protection Officer and the Network Manager are responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members after discussions with the IT Lead for SLT and the Headteacher.

Useful Contact information

ICO Helpline	**0303 123 1113**
B&NES IT Services	**01225 477199**
Integra SIMS Support	**01454 865300**

St Gregory’s Timeline of Breach or Data Protection Incident Management

Date	Time	Reported by	Brief Description	Investigated by	Reported to ICO Yes/ No