The Holt School
Data Security Breach Prevention and Management Policy

May 2018

Version	DATE	DESCRIPTION
1	May 2018	New policy – GDPR compliant

Reviewed	May 2018
Responsibility	Mrs J Perry
Committee	Finance & Premises
Review Date	May 2020

Contents:

Statement of intent

The Holt School 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.

For the purposes of this policy, the title of ‘data controller’ will be used in reference to the person(s) primarily responsible for the handling and protection of information and data within a school i.e the schools IT Support provider.

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 1998
- 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:

- E-Safety Policy
- Data Protection Policy
- Acceptable Use Policy

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 Data Protection Officer 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 data controller is responsible for the overall monitoring and management of data security.

3.3. The Data Protection Officer is responsible for establishing a procedure for managing and logging incidents.

3.4. The governing body is responsible for holding regular meetings with the Co-Headteachers and Data Protection Officer to discuss the effectiveness of data security, and to review incident logs.

3.5. All members of staff and pupils are responsible for adhering to the processes outlined in this policy, alongside the school's E-Safety Policy and Acceptable Use 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 finance office and will be audited on an annual basis to 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 Data Protection Officer before use.

4.3. All systems will be audited on a termly basis 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 on an annual basis 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.

5. Network security

5.1. The school will employ firewalls in order to prevent unauthorised access to the systems.

5.2. The school's firewall will be deployed as a:

- **Centralised deployment**: the broadband service connects to a firewall that is located within a data centre or other major network location.

5.3. As the school's firewall is managed locally by a third party, the firewall management service will be thoroughly investigated by the I.T Support provider to ensure that:

- Any changes and updates that are logged by authorised users within the school are undertaken efficiently by the provider to maintain operational effectiveness.
- Patches and fixes are applied quickly to ensure that the network security is not compromised.

5.4. The school will consider installing additional firewalls on the servers in addition to the third-party service as a means of extra network protection. This decision will be made by the Co-Headteachers, taking into account the level of security currently provided and any incidents that have occurred.

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 Data controller will ensure that all school devices have secure malware protection and undergo regular malware scans.

6.3. The Data controller will update malware protection on a termly basis to ensure it is up-to-date and can react to changing threats.

6.4. Malware protection will also be updated in the event of any attacks to the school's hardware and software.

6.5. 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 Data controller.

6.6. The school will use 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.

6.7. The Data controller 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. User privileges will be differentiated, i.e. pupils will have different access to data and the network than members of staff.

7.2. The Co-Headteachers will clearly define what users have access to and will communicate this to the data controller, ensuring that a written record is kept.

7.3. The data controller will ensure that user accounts are set up to allow users access to the facilities required, in line with the Co-Headteachers's instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

7.4. All users will be required to change their passwords on an annual basis and must use upper and lowercase letters, as well as numbers, to ensure that passwords are strong. Users will also be required to change their password if they become known to other individuals.

7.5. Pupils are responsible for remembering their passwords; however, the data controller will have an up-to-date record of all usernames and will be able to help reset passwords if necessary.

7.6. Automated user provisioning systems will be employed in order to automatically delete inactive users or users who have left the school. The data controller will manage this provision to ensure that all users that should be deleted are, and that they do not have access to the system.

7.7. The data controller will review the system on a termly basis to ensure the system is working at the required level.

8. Removable media controls and home working

8.1. The school understands that pupils 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.

8.2. The data controller will encrypt all school-owned devices for personal use, such as laptops, USB sticks, mobile phones and tablets, to ensure that they are

password protected. If any portable devices are lost, this will prevent unauthorised access to personal data.

8.3. Pupils and staff are not permitted to use their personal devices where the school shall provide alternatives, such as work laptops, tablets and USB sticks, unless instructed otherwise by the Co-Headteachers.

8.4. If pupils 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 data controller.

8.5. When using laptops, tablets and other portable devices, the Co-Headteachers will determine the limitations for access to the network, as described in section 5 of this policy.

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

8.7. The data controller will use encryption to filter the use of websites on these devices, in order to prevent inappropriate use and external threats which may compromise network security when bringing the device back onto the premises.

8.8. The school uses tracking technology where possible to ensure that lost or stolen devices can be retrieved.

8.9. 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.

8.10. The Wi-Fi network at the school will be password protected and will only be given out as required. Staff and pupils are not permitted to use the Wi-Fi for their personal devices, such as mobile phones or tablets, unless instructed otherwise by the Co-Headteachers.

8.11. A separate Wi-Fi network will be established for visitors at the school to limit their access to printers, shared storage areas and any other applications which are not necessary.

9. Backing-up data

9.1. The data controller performs a back-up of all electronic data held by the school on a daily basis, and the date of the back-up is recorded using a log. Each back-up is retained for up to three months before being deleted.

9.2. Back-ups are run overnight and are completed before the beginning of the next school day.

9.3. Upon completion of back-ups, data is stored on the school's hardware which is password protected.

9.4. Data is also replicated weekly and stored offsite on a Network Attached Storage device (encrypted drive)

9.5. Only authorised personnel are able to access the school's data.

10. User training and awareness

10.1. The data controller and Co-Headteachers will arrange training for pupils and staff on an annual basis to ensure they are aware of how to use the network appropriately in accordance with the Acceptable Use Policy and E-Safety Policy.

10.2. Training for all staff members will be arranged by the data controller within two weeks following an attack or significant update.

10.3. Through training, all pupils 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.

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

10.5. 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 E-Safety Policy.

11. Security breach incidents

11.1. Any individual that discovers a security data breach will report this immediately to the Co-Headteachers and data controller.

11.2. When an incident is raised, 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

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

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

11.5. The Data Protection Officer will oversee a full investigation and produce a comprehensive report.

11.6. 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.

11.7. If the Data Protection Officer determines that the severity of the security breach is low, the incident will be managed in accordance with the following procedures:

- In the event of an internal breach, the incident is recorded using an incident log, and by identifying the user and the website or service they were trying to access.
- The Co-Headteachers will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.
- The data controller will work with the third-party provider to provide an appropriate response to the attack, including any in-house changes.

11.8. 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.

11.9. 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.

11.10. Where appropriate, e.g. if offences have been committed under the Computer Misuse Act 1990, the Data Protection Officer will inform the police of the security breach.

11.11. The data controller 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.

12. Assessment of risks

12.1. The following questions will be considered by the data controller 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 controller's report and records:

- What type and how much data is involved?
- How sensitive is the data? Sensitive data is defined in the Data Protection Act 1998; 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 pupils, 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?

12.2. In the event that the data controller and Data Protection Officer, 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).

13. Consideration of further notification

13.1. 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).

13.2. The school will decide whether notification will help the school meet its security obligations under the seventh data protection principle.

13.3. 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.

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

13.5. 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.

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

13.7. 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:

13.8. 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.

13.9. 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.

13.10. 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, pupils 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 Protection Officer 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.

14. Evaluation and response

14.1. The data controller and Data protection Officer will establish the root of the breach, and where any present or future risks lie.

14.2. The data controller and Data protection Officer will consider the data and contexts involved.

14.3. The data controller and Data protection Officer will identify any weak points in existing security measures and procedures.

14.4. The data controller and Data protection Officer will identify any weak points in levels of security awareness and training.

14.5. The data controller and Data protection Officer will report on findings and, with the approval of the school leadership team, implement the recommendations of the report after analysis and discussion.

15. Monitoring and review

15.1. This policy will be reviewed by the Co-Headteachers, in conjunction with the data controller and Data protection Officer, on an biennial basis.

15.2. The Data Protection Officer is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date