Altwood
Church of England School

E-Security Policy

Breach Prevention and Management Plan

Next review June 2023

E-Security Policy
Breach Prevention and Management Plan

Altwood
Church of England School

Contents:

E-Security Policy
Breach Prevention and Management Plan

Altwood
Church of England School

Statement of intent

At Altwood Church of England School, we understand that use of the internet and broadband is important for day-to-day activities and for enhancing the learning of our pupils, which, if not properly managed, drastically increases the chance of harm to pupils, staff and Governors.

The 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 most of the 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 procedure 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 about the person primarily responsible for the handling and protection of information and data within a school.

This policy applies to all Governors, staff, and volunteers working for the school either remotely or on site.

E-Security Policy
Breach Prevention and Management Plan

Altwood
Church of England School

1. Legal framework

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

- The Human Rights Act 1998
- The Data Protection Act 2018 (also GDPR 2018)
- The regulation of investigatory Powers Act 2000
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspections Act 2006
- The Computer Misuse Act 1990

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

- GDPR Policy
- Acceptable Use Guidance

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/Data theft** – 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 IT 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 because 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. because of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data.
- Negligence, e.g. because 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 data controller is responsible for the overall monitoring and management of data security.

3.3. The data controller is responsible for establishing a procedure for managing and logging incidents.

3.4. The governing body is responsible for reviewing incidents which will be shared with them by the data controller as they occur.

3.5. All Governors, staff, volunteers and pupils are responsible for adhering to the processes outlined in this 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 securely and electronically and will be regularly backed up and will be audited on a termly 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 controller 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 every 90 days to prevent access to facilities which could compromise network security.

4.6. The school believes that locking down hardware, such as using strong passwords, is an effective way to prevent access to facilities by unauthorised users.

5. Network security

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

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

- **Localised deployment**: the broadband service connects to a firewall that is located on an appliance or system on the school premises, as either discrete technology or a component of another system.

5.3. As the school's firewall is managed on the premises, it is the responsibility of the data controller to effectively manage the firewall. The data controller will ensure that:

- The firewall is checked weekly for any changes and/or updates, and that these are recorded using the inventory.
- Any changes and/or updates that are added to servers, including access to new services and applications, are checked to ensure that they do not compromise the overall network security.
- The firewall is checked weekly to ensure that a high level of security is maintained and there is effective protection from external threats.
- Any compromise of security through the firewall is recorded using an incident log and is reported to the headteacher. The data controller will react to security threats to find new ways of managing the firewall.

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 IT Technician will update malware protection as required when updates are provided 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 IT technician will review the mail security technology on a weekly 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 headteacher 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 headteachers instructions, whilst minimising the potential for deliberate or accidental attacks on the network.

7.4. The data controller will ensure that websites are constantly being filtered for inappropriate and malicious content. Any member of staff or pupil that has accessed inappropriate or malicious content will be recorded in accordance with the monitoring process in section 8 of this policy.

7.5. All users will be required to change their passwords every 90 days 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.

7.6. Pupils are responsible for remembering their passwords; however, the IT Technician will be able to reset them if necessary.

7.7. The 'master user' password list will be maintained by the IT Technician and made available to the data controller/headteacher or nominated senior leader, and will be stored securely on the school network.

7.8. A multi-user account will be created for visitors to the school, such as volunteers, and access will be filtered as per the headteacher's instructions. Usernames and passwords for this account will be changed on a termly basis, and will be provided as required.

7.9. 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.

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

8. Monitoring usage

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

8.2. The school will inform all pupils and staff that their use of school IT equipment and systems will be monitored and recorded.

8.3. If a user accesses inappropriate content or a threat is detected, an Impero alert will be sent to the data controller, some member of SLT and the IT Technician. Alerts will also be sent for unauthorised and accidental usage.

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. All incidents will be responded to in accordance with section 12 of this policy.

8.6. All data gathered by monitoring usage will be kept electronically and securely. 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.

8.7. False positive reports will be deleted.

9. Removable media controls and home working

9.1. 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.

9.2. The IT Technician 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.

9.3. 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 headteacher.

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

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

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

9.7. The Wi-Fi network at the school will be password protected and will only be given out as required.

9.8. Staff and pupils may only use the BYOD Wi-Fi System to connect their personal devices, such as mobile phones or tablets.

9.9. 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.

10. Backing-up data

10.1. The data controller will ensure that there are two backups of all electronic data held by the school. The backup servers will be located onsite but in separate buildings. The first server (located in Admin) will perform a nightly incremental backup of all Altwood data.

10.2. The data controller will ensure that a second full back is completed twice weekly on the server located in the Winchester building. This server will remain offline other than to complete the back up and will then shut down automatically. This is to limit the potential corruption of the backup via ransomware threats.

10.3. Back up management is by VEEAM and reports are automatically generated to show completion and or errors. These are then sent by email to the data controller and IT technician.

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

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

10.6. User data is also stored via One Drive by Microsoft.

10.7. Only authorised personnel can access the school's data.

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

10.9. The data controller performs an incremental back-up on a monthly basis of any data that has changed since the previous back-up. The data controller will record the date of any incremental back-up, alongside a list of the files that have been included in the back-up.

10.10. Where possible, back-ups are run overnight and are completed before the beginning of the next school day.

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

10.12. Data is also replicated and stored in accordance with the school's Cloud Computing Policy.

10.13. Only authorised personnel can access the school's data.

11.User training and awareness

11.1. The data controller and headteacher will arrange training for pupils and staff as appropriate.

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

11.3. Through training, all pupils and staff will be aware of who they should inform first if 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 pupils 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 E-Safety Policy.

12.Security breach incidents

12.1. Any individual that discovers a security data breach will report this immediately to the headteacher and data controller.

12.2. When an incident is raised, the headteacher 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 data controller will take the lead in investigating the breach and will be allocated the appropriate time and resources to conduct this.

12.4. The data controller, 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 controller will oversee a full investigation and produce a comprehensive report.

12.6. The cause of the breach, and whether 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 controller 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 headteacher will issue disciplinary sanctions to the pupil or member of staff, in accordance with the processes outlined in the E-safety Policy.
- In the event of any external or internal breach, the data controller will record this using an incident log and respond appropriately, e.g. by

updating the firewall, changing usernames and passwords, updating filtered websites or creating further back-ups of information.

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 data controller will inform the police of the security breach.

12.11. 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.

13.Assessment of risks

13.1. The following questions will be considered by the data controller 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 was 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?

13.2. In the event that the data controller, 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 decide whether notification will help the school meet its security obligations under the seventh data protection principle.

14.3. 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.

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

14.5. 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.

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

14.7. 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:

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

14.9. The school will use the timeline in Appendix B to record events.

14.10. 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.

14.11. 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 controller 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 data controller will establish the root of the breach, and where any present or future risks lie.

15.2. The data controller will consider the data and contexts involved.

15.3. The data controller and headteacher will identify any weak points in existing security measures and procedures.

15.4. The data controller and headteacher will identify any weak points in levels of security awareness and training.

15.5. The data controller 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 controller, on an annual basis.

16.2. The data controller is responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

Appendix A

1. Organisation details

a What is the name of your organisation- is it the data controller in respect of the breach?

b Please provide the data controllers registration number.

Search the online data protection public register

c Who should we contact if we require further details concerning the incident? (Name and job title, email address, contact telephone number and postal address

2. Details of the data protection breach

a. Please describe the incident in as much detail as possible

b. When did the incident happen?

c. How did the incident happen?

d. If there has been a delay in reporting the incident to the ICO please explain your reasons for this.

e. What measurers did the organisation have in place to prevent an incident of this nature occurring?

f. Please provide extracts of any policies and procedures considered relevant to this incident, and explain which of these were in existence at the time this incident occurred. Please provide the dates on which they were implemented

3. Personal data placed at risk

What personal data has been placed at risk? Please specify if any financial or sensitive personal data has been affected and provide details of the extent.

How many individuals have been affected?

Are the affected individuals aware that the incident has occurred?

What are the potential consequences and adverse effects on those individuals?

Have any affected individuals complained to the organisation about the incident?

4. Containment and recovery

a. Has the organisation taken any action to minimise/ mitigate the effect on the affected individuals? If so, please provide details

b. Has the data place at risk now been recovered? If so, please provide details of how and when this occurred

c. What steps has your organisation taken to prevent a recurrence of this incident?

5. Training and guidance

a. As the data controller, does the organisation provide its staff with training on the requirements of the Data Protection Act? If so, please provide any extracts relevant to this incident here.

b. Please confirm if training is mandatory for all staff. Had the staff members involved in this incident received training and if so when?

c. As the data controller, does the organisation provide any detailed guidance to staff on the handling of personal data in relation to the incident you are reporting? If so, please provide any extracts relevant to this incident here.

6. Previous contact with the ICO

a. Have you reported any previous incidents to the ICO in the last two years?

b. If the answer to the above question is yes, please provide: brief details, the date on which the matter was reported and, where known, the ICO reference number.

7. Miscellaneous

a. Have you notified any other (overseas) data protection authorities about this incident? If so, please provide details

b. Have you informed the Police about this incident? If so, please provide further details and specify the Force concerned.

c. Have you informed any other regulatory bodies about this incident? If so please provide details.

d. Has there been any media coverage of the incident? If so, please provide details of this.

Sending this form

Send your completed form to casework@ico.org.uk, with ‘DPA breach notification form’ in the subject field, or by post to: The Information Commissioner’s Office, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Please note that we cannot guarantee security of forms or any attachments sent by email.

What happens next?

When we receive this form, we will contact you within seven calendar days to provide:

- a case reference number; and
- information about our next steps

If you need any help in completing this form, please contact our helpline on
0303 123 1113 or **01625 545745** (operates 9am to 5pm Monday to Friday)

Submitted By

Signature: …………………………………………..

Name: ……………………………………………….

Title: Data Controller

Date: ………………………….

Appendix B

Timeline of Incident Management

Date	Time	Activity	Decision	Name/position	Date