and

# Abbots Farm Preschool

## Cyber Security Policy

**March 2026**

**Review by March 2027**

## Contents

# Statement of Intent

Abbots Farm Infant School and Abbots Farm Preschool are committed to maintaining the confidentiality, integrity and availability of its information and ensuring that the details of the finances, operations and individuals within the school are only accessible to the appropriate individuals. It is, therefore, important to implement appropriate levels of access, uphold high standards of security, take suitable precautions, and have systems and procedures in place that support this.

This Policy applies to:

- All members of staff and governors; “Staff” includes all employees, locum staff, volunteers, work experience and any other individuals working for Abbots Farm Infant School and Abbots Farm Preschool on a contractual basis.

The importance of this Policy:

- This Cyber Security Policy lets you know what your responsibilities are at Abbots Farm Infant School and Abbots Farm Preschool; everyone has a role to play and it’s vital you understand yours.

The objective of this Policy is to:

- Inform staff and governors and protect Abbots Farm Infant School and Abbots Farm Preschool from security issues that might have an adverse impact on our organisation. Achieving this objective will rely on all staff and governors of the schools complying with this policy.

**Abbots Farm Infant School and Abbots Farm Preschool have adopted the following six principles to underpin its Cyber Security Policy:**

All personal data shall be:

(1) processed lawfully, fairly and in a transparent manner ('lawfulness, fairness and transparency');

(2) used for specified, explicit and legitimate purposes ('purpose limitation');

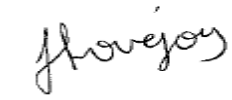
(3) used in a way that is adequate, relevant and limited to what is necessary ('data minimisation');

(4) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, are erased or rectified without delay ('accuracy');

(5) kept no longer than is necessary ('storage limitation');

(6) processed in a manner that ensures it is safe and secure, ensuring that measures against unauthorised or unlawful processing and against accidental loss, destruction or damage are in place ('integrity and confidentiality').

Signed by:



Headteacher Date: 20/1/26

Chair of governors Date: 20/1/26

# 1. Legal framework

This policy has due regard to all relevant legislation and guidance including, but not limited to, the following:

- Computer Misuse Act 1990
- The UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- National Cyber Security Centre (2018) 'Small Business Guide: Cyber Security'
- National Cyber Security Centre (N.D.) 'Cyber Essentials'
- ICO (2022) 'Guide to the UK General Data Protection Regulation (GDPR)'
- (DfE) (2025) 'Meeting digital and technology standards in schools and colleges'

This policy operates in conjunction with the following school policies and procedures:

- Behaviour and Relationships Policy
- Data Protection Policy
- Data Retention Policy
- Online Safety Policy
- Remote Education Plan
- WCC Disciplinary Policy and Procedure
- Cyber Response and Recovery Plan

# 2. Types of security breach and causes

**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. This includes unauthorised people within the school, e.g. schools where pupils access systems that staff have left open and/or logged in, or where staff access data beyond their authorisation, as can occur in schools where all staff are given admin-level access for ease.

**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.

**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.

**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.

Breaches in security may be caused by the actions of individuals, and may be accidental, malicious or the result of negligence:

- Accidental breaches can occur as a result of human error or insufficient training for staff, so they are unaware of the procedures to follow
- Malicious breaches can occur as a result of a hacker wishing to cause damage to the school through accessing and altering, sharing or removing data

Breaches caused by negligence can occur as a result of a staff member knowingly disregarding school policies and procedures or allowing pupils to access data without authorisation and/or supervision

Breaches in security may also be caused by system issues, which could involve incorrect installation, configuration problems or operational errors:

- The incorrect installation of antivirus software and/or use of outdated software can make the school software more vulnerable to a virus
- Incorrect firewall settings being applied, e.g. unrestricted access to the school network, can allow unauthorised individuals to access the school system

Operational errors, such as confusion between back-up copies of data, can cause the most recent data to be overwritten

# 3. Roles and responsibilities

The **Governing Body** will be responsible for:

- Ensuring the school has appropriate cyber-security measures in place.
- Ensuring the school has an appropriate approach to managing data breaches in place.
- Supporting the headteacher and other relevant staff in the delivery of this policy.
- Ensuring the school meets the relevant cyber-security standards.
- Ensuring at least one member of the board completes basic cyber-security training.

The **Headteacher** will be responsible for:

- Ensuring all staff members and pupils are aware of their responsibilities in relation to this policy.
- Ensuring appropriate user access procedures are in place.
- Responding to alerts for access to inappropriate content in line with the Online Safety Policy.
- Organising training for staff members.
- Leading on the school's response to incidents of data security breaches
- Determining which organisations and individuals need to be notified following a data security breach, and ensuring they are notified.
- Ensuring a log of cyber security incidents is maintained.
- Determining where weaknesses lie and improve security measures after a data security breach
- Supporting the local authority (LA) ICT Development Service (ICTDS) cyber recovery team if needed.
- Maintaining an inventory of all ICT hardware and software currently in use at the school.
- Ensuring any out-of-date software is removed from the school systems.
- Liaising with ICTDS to implement effective firewalls and filtering systems to enhance network security and ensuring that these are monitored regularly.
- Setting up user privileges in line with job roles.
- Maintaining an up-to-date and secure inventory of all usernames and passwords.
- Removing any inactive users from the school system and ensuring that this is always up-to-date.
- Ensuring ICTDS are performing a back-up of all electronic data held by the school.

- Ensuring all school-owned devices have secure malware protection and are regularly updated.
- Recording any alerts for access to inappropriate content.
- Monitoring and reviewing the effectiveness of this policy

The **Online Safety Lead** will be responsible for:

- Organising training and resources for staff on online safeguarding risks and preventative measures.
- Taking responsibility for online safety within the school and promoting online safety measures to parents.
- Ensuring the relevant policies and procedures are in place to protect pupils from harm, including the Online Safety Policy.
- Monitoring online safety incidents which could result in data breaches and reporting these to the Data Protection Champion.
- Acting as the named point of contact within the school on all online safety issues.
- Liaising with relevant members of staff on online safety matters, e.g. the Data Protection Champion and ICT technician.

All **staff members** will be responsible for:

- Understanding their responsibilities in regard to this policy.
- Undertaking the appropriate training.
- Ensuring they are aware of when new updates become available and how to safely install them.

# 4. Creating, storing and managing information

Abbots Farm Infant School and Abbots Farm Preschool have adopted both a clear desk and clear screen practices to reduce the risks of unauthorised access to, loss of, and damage to information during and outside normal working hours or when work areas and computers are unattended.

This section explains the school's requirements to ensure that information is not disclosed by being made available in any form to unauthorised individuals.

**Paper information**

- Keep clear desks as this is an obvious way of preventing any confidentiality problems arising from having pupils or other staff members at desks, or disclosure when desks are left unattended. A clear desk will help to protect against the disclosure of information.
- Confidential documents must not be left on display or unsupervised.
- Store confidential information in locked cabinets, returning them to these cabinets when not required.
- Take measures to prevent accidental damage to important documents, for example, through the spillage of liquids.
- Do not leave paper by printers or photocopiers where other people may take it or read it accidentally.

- Spoiled photocopies and prints of a confidential nature are disposed of by shredding as outlined in the Data Protection Policy. Always check that originals have been removed from the device as well as copies.
- Dispose of confidential paper by shredding. Do not dispose of confidential waste in a waste paper bin or anywhere else.
- Destroying information earlier than necessary may be a breach of the law so it is important that retention periods are checked before destroying any records.

### Electronic information

- All confidential information must be stored on Abbots Farm Infant School and Abbots Farm Preschool approved electronic devices or systems with access controlled/restricted, e.g. the school network, cloud storage with appropriate restricted access
- Confidential information must not be stored on local unencrypted hard drives.
- If confidential information has to be transferred to other portable media, such as USB stick or memory cards, it must be encrypted with appropriate security software approved by Abbots Farm Infant School and Abbots Farm Preschool.
- PC screens/laptops/tablets must be sited away from public areas so that pupils and visitors cannot read the screens, e.g. through windows or while waiting in public areas.
- Laptops, Chromebooks, handhelds or any other portable ICT devices must not be left unattended in any public area
- Individual user id/passwords must not be shared with anyone, including other staff members and governors, and do not use anyone else's password. You as an individual are responsible for all transactions undertaken on the school network using your network id.
- Passwords must not be written down and left with any equipment or accessible by anyone else.
- Make passwords hard for anyone else to guess by incorporating numbers and mixed case into it. Some systems will force this already.
- It is recommended that staff change their passwords half-termly.
- Lock screens whenever leaving any ICT equipment unattended. This will prevent anyone accessing any restricted information on the equipment while it is unattended.
- If you find you have access to confidential information that you believe should be restricted, you should notify **Jeanette Lovejoy (Headteacher) / Lydia Mortimer (SBM)** immediately.

## 5. Receiving, sending and sharing information

### Post – receiving and sending

- Post should be opened and dealt with away from public areas and securely, if dealing with confidential information. Do not leave unsealed confidential documents in open post trays and 'pigeon holes'.
- Staff must ensure that any mail to an individual marked: Private, Confidential or Personal, or any combination, is only passed to the named recipient unless a prior delegation arrangement has been made.
- If outgoing post contains confidential information to an individual, the envelope should be marked as 'Private and confidential' and 'to be opened by addressee only'.

A return address must be shown on the envelope and you should consider double bagging the package.

- Print each letter separately making use of any printing security and use window envelopes. Check the address is the current, correct one – don't copy previous letters. Double check that the letter and papers are for the correct recipient and address.
- When using a mailshot or multiple mailings, have a procedure in place to check you haven't included anyone else's personal information in the wrong envelope. Another person or supervisor should check mailings against address lists and sign-off before dispatch.
- Use signed for/tracked post, if it contains sensitive or confidential documents and/or the volume justifies secure delivery.
- Post containing very high risk/Confidential-Restricted information should only be sent to a named person and use of tracked and signed for mail or a courier to deliver to the name person with signature of receipt.
- If post goes astray or is issued to the incorrect address, notify your line manager immediately and if the information contains personal or confidential information report using the security incident procedure.

## Email and Other Electronic Communications (e.g. text messages) – receiving and sending

- Abbots Farm Infant School and Abbots Farm Preschool do not have total control over emails received, so staff must be aware of the dangers of opening messages from unknown or untrusted sources. Do not click on links in emails unless you know they are from a trusted source and never provide passwords in response to email requests.
- If you are not the intended recipient, the sender should be informed that the message has not reached its intended destination and has been deleted.
- Check the email address is the correct one – there are staff with similar names and your email contacts will also have external email contacts. Double check that the email is for the correct recipient before sending.
- If sending to a list/group of parents or others, send using 'blind copy' (bcc) so the recipients are not copied in to a large list. This especially applies to mailshots.
- Confidential and Confidential-Restricted information must not be emailed externally using normal email unless;

a) you are using an encrypted email service provided by Abbots Farm Infant School and Abbots Farm Preschool, or

b) the information is encrypted / password protected in an attachment, or

c) you are sending to an approved school email address, e.g. a school welearn email address, or

d) you are sending to an e-mail address which utilises the same server – for schools which use the 'welearn' e-mail system this includes all other schools with this system as well as Warwickshire County Council.

- Records of personal data sent by email or other electronic communications (internal or external) are accessible to the data subject if they request access under the

GDPR. If a permanent record is required they should be saved to the appropriate file and the email removed from the email inbox. Do not use personal email as a permanent filing system for pupil, parent or staff records. When a member of staff leaves or moves to another job, the line manager must go through the Leavers Checklist and save and secure any emails needed to be kept as Abbots Farm Infant School and Abbots Farm Preschool records.

- School confidential emails must not be forwarded to your own personal email account for private use.

## Telephone calls

- Ensure that you are talking to who you think you are speaking with by verifying their details. It may be appropriate to call them back to verify their credentials.
- If it becomes necessary to leave the phone for any reason, put the caller on hold so that they cannot hear other potentially confidential conversations that may be going on in the office.
- If the call received or being made is of a confidential or sensitive nature, consider who else may be listening to the conversation.
- If a message needs to be taken and left on someone's desk, ensure that these messages do not themselves contain confidential information.
- Do not leave confidential messages on an answer machine as these can be reviewed by people other than the intended person.

## Conversations

Staff should remember that even though they may be on Abbots Farm Infant School and Abbots Farm Preschool premises there may be pupils and visitors around.

- When having a meeting or interview with someone where confidential information will be discussed, ensure that there is sufficient privacy. Check that the room is suitable.
- Confidential information should only be discussed with colleagues who need to know the information in order to carry out their job.
- Always consider your surroundings and the proximity of others who may be able to hear in public places.

## Information sharing/processing

When confidential or personal data is shared with other agencies, for example with local authorities or external providers, then arrangements must be made for that information sharing to be done in a controlled way that meets ethical and legal obligations in one of two ways:

1. If a service is commissioned with an external provider that needs confidential information to operate then the contract must contain clauses that list the commissioned organisation's responsibilities for confidential and personal data, including data protection and security. This must include whether the organisation is processing personal data on behalf of Abbots Farm Infant School and Abbots Farm Preschool or has sole or joint responsibilities for the personal data with the schools. All staff involved in such data commissioning/sharing must be aware of the details of any existing information sharing agreements/contractual agreements and the obligations that it places on them.

2. If information has to be shared with another organisation on a regular basis for legal reasons then this should be done under an information sharing agreement that sets out how

the sharing will operate and the standards of management that all parties to the agreement must comply with. Such an agreement will define exactly what information will be shared and how, including the method, transmission or communication between agencies or any shared access security arrangements. The aim is to ensure that appropriate arrangements operate in the participant agencies and ensure the continued confidentiality of shared information. If staff are unclear on what basis information is being shared with another agency, whether an information agreement exists and what obligations that might place on them, it should be clarified with their manager.

# 6. Working Away from School

The purpose of this section is to ensure that information assets and information processing facilities, used to access personal and confidential information, are adequately protected with logical, physical and environmental controls.

This includes working away from the school, at home and use of own devices to access personal and confidential information.

Work-related information must not be kept permanently at home. Wherever staff are working on, or in possession of, work-related information they are responsible for it, e.g. in school, on the phone, at home, en route to or from school or home, at meetings, conferences, etc. If confidential information is handed out in conferences or meetings, the same person is responsible for collecting it back in at the end, or ensuring it is only in the hands of those authorised to keep it.

- Take only the confidential papers/files with you that you need and keep out of sight in a bag; do not carry around loose or in clear folder.
- Managers must ensure a log is kept of which confidential paper case files/records staff are taking from school and when they are returned.
- Store confidential paper files/records securely in an envelope or bag. Try to use electronic files on an encrypted device or access via secure connection to the network or approved storage location instead.
- Keeping information in cars: lock away paper files and equipment (laptop/notebook) in the boot, do not leave overnight. Take only the equipment/papers/files with you that you need, leave rest locked away.
- Travelling by public transport: make sure you take all information and equipment when leaving. Be aware of conversations on mobile phone about personal and confidential information.
- Use of Laptops: Only school issued devices may be used. Do not write down passwords/Pins. You must not use the ‘remember me’ option to save user and password details on your device when accessing Abbots Farm Infant School and Abbots Farm Preschool system. Make sure these are unticked and sign out/logout after using a system. Do not save login or passwords if asked. Remember any confidential files opened may be downloaded before closing down your device, so delete them from ‘downloads’. If files are not accessed directly (e.g. cloud storage), then all confidential files must be stored and accessed locally via a school-approved encrypted media.
- Working at home: Store paper and equipment securely after use, as you would your own personal valuables. Don’t leave open confidential files on a table. Lock screen on laptop/tablet and close down after use. All confidential information must be safeguarded from access, no matter how unintentional, by anyone who has no need

to know such as family and friends. This would be an unauthorised disclosure. Don't leave any school equipment or information in a car overnight at home, bring into the house and secure. Don't bin confidential information at home, bring back into an office for confidential waste disposal. Use strong security on a home Wi-Fi connection.

# 7. Removable media controls

The school understands that staff may need to access the school network from outside the school premises. Effective security management will be established to prevent access to, or leakage of, data, as well as any possible risk of malware. These are the control requirements for the use of removable media devices within and across Abbots Farm Infant School and Abbots Farm Preschool. Portable media devices include, but are not limited to, USB sticks.

- Connection of non-school supplied removable media devices to the school's computing infrastructure is only permitted for the purpose of reading files from the device; School files must not be written to a non-school supplied device.
- Staff must not alter or disable any controls applied to any computing device by school IT Service as part of the deployment of a removable media device.
- Removable media devices must not be used for the primary long-term storage of school information.
- All information of a confidential or personal nature that is stored on a removable media device must be encrypted.
- Passwords applied to encrypted devices must conform to the minimum standard required stated in section Electronic Information of this Policy.

Staff who use school-owned laptops, tablets and other portable devices will use them for work purposes only, whether on or off the school premises. Staff will avoid connecting to unknown Wi-Fi hotspots, such as in coffee shops, when using any school-owned laptops, tablets or other devices, or when accessing school networks.

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 agreed prior to usage. A separate Wi-Fi network (BYOND) is established for visitors at the school to limit their access to school networks and any other applications which it is not necessary for them to access.

# 8. Malware prevention

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, malicious websites or removable media controls. The purpose of this section is to establish requirements, which must be met by all devices within Abbots Farm Infant School and Abbots Farm Preschool's computing infrastructure, to protect the confidentiality, integrity and availability of school software and information assets from the effects of malware.

- Unless undertaken by or following instruction from Headteacher or LA IT support staff, staff must not disable anti-malware software running on, or prevent updates being applied to devices.
- The intentional introduction of viruses to school's computing infrastructure will be regarded as a serious disciplinary matter.

- Only software that has been authorised by school can be installed upon school systems.
- Each member of staff is responsible for immediately reporting any abnormal behaviour of school computing systems to Warwickshire IT service desk.
- Prior to any encryption, all files must be scanned for and cleaned of viruses before being sent to any third party.

Staff will follow procedures for filtering and monitoring to keep pupils safe as set out in the Online Safety Policy.

Filtering of websites will ensure that access to websites with known malware are blocked immediately.

# 9. User privileges and passwords

The school understands that controlling what users have access to is important for promoting network security and data protection. User privileges will be differentiated, e.g. pupils will have different access to data and the network than members of staff, whose access will also be role-based.

The headteacher will clearly define what users have access to and will ensure that user accounts are set up to allow users access to the facilities required.

- Access to information shall be restricted to users who have an authorised need to access the information.
- Users of information will have no more access privileges than necessary to be able to fulfil their role.
- All requests for access to Abbots Farm Infant School and Abbots Farm Preschool computer systems must be via a formal request to the Headteacher.
- School reserves the right to revoke access to any or all of its computer systems at any time.
- Users must not circumvent the permissions granted to their accounts in order to gain unauthorised access to information resources.
- Users must not allow anyone else to use their account, or use their computers while logged in with their account.
- Computer screens should be 'locked' or the user logged out before leaving any workstation or device unattended.

All users will be required to change their passwords on an annual basis and/or if they become known to other individuals. The Headteacher and School Business Manager will have an up-to-date record of all usernames and will be able to reset them if necessary.

A multi-user account will be created for visitors to the school, such as volunteers, and access will be filtered by the Headteacher. Passwords for this account will be changed on a weekly basis and will be provided as required.

The school will implement a user account creation, approval and removal process which is part of the school joining and leaving protocols. The Headteacher will delete inactive users or users who have left the school to ensure that they do not have access to the system.

User accounts and access privileges will be appropriately controlled, and only authorised individuals will have an account which enables them to access, alter, disclose or delete personal data. Users will have a separate account for routine business if their main account:

- Is an administrative account.
- Enables the execution of software that makes significant system or security changes.
- Can make changes to the operating system.
- Can create new accounts.
- Can change the privileges of existing accounts.

# 10. Monitoring System Access and Use

Monitoring user activity is important for the early detection of attacks and incidents, as well as inappropriate usage by pupils or staff. The school informs all pupils and staff that their usage will be monitored, as well as how it is being monitored and why, in accordance with the school's Online Safety Policy. Smoothwall and RADAR is used for web filtering.

If a user accesses inappropriate content or a threat is detected, an alert will be sent to the Headteacher. Alerts will identify the user, the activity that prompted the alert, and the information or service the user was attempting to access. All incidents will be responded to in accordance with the 'Data security breach incidents' section of this policy, and as outlined in the Online Safety Policy.

An audit trail of system access and staff data use shall be maintained and reviewed on a regular basis. School will put in place routines to regularly audit compliance with this and other policies. In addition it reserves the right to monitor activity where it suspects that there has been a breach of policy.

Any monitoring will be undertaken in accordance with the Human Rights Act and any other applicable law.

# 11. Home working

Staff will adhere to data protection legislation and the school's related policies when working remotely.

Staff will receive annual training regarding what to do if a data protection issue arises from any home working.

Wherever possible, personal data will not be taken home by staff members for the purposes of home working, due to the risk of data being lost or the occurrence of a data breach.

Staff are not permitted to let their family members or friends use any school equipment, in order to protect the confidentiality of any personal data held on the device. Any staff member found to have shared personal data without authorisation will be disciplined in line with the Disciplinary Policy and Procedure. This may also result in a data breach that the school would need to record and potentially report to the ICO.

Staff who require access to personal data to enable them to work from home will first seek approval from the headteacher, and it will be ensured that the appropriate security measures are in place e.g. secure passwords and anti-virus software.

Staff will be informed that caution should be exercised while accessing personal data if an unauthorised person is in the same room. If a member of staff needs to leave their device unattended, the device should be locked. School devices will automatically lock after one minute of inactivity to avoid an unauthorised person gaining access to the device.

To ensure reasonable precautions are taken when managing data, staff will avoid:

- Keeping personal data on unencrypted hard drives.
- Sending work emails to and from personal email addresses.
- Leaving logged-in devices and files unattended.
- Using shared home devices where other household members can access personal data.
- Using an unsecured Wi-Fi network.

Staff working from home will be encouraged and enabled to go paperless, where possible, as paper files cannot be protected digitally and may be misplaced. If sensitive data is taken off the school premises to allow staff to work from home, it will be transported in a bag or folder that is opaque. The school's procedures for taking data off the school premises will apply to both paper-based and electronic data.

When taking physical copies of data, e.g. paper documents and school-owned devices, off the school premises, staff will sign out the documents at the school office. The physical data will be signed back in when staff return it.

In the event that a staff member decides to leave the school permanently, all devices and data in any form will be returned on or before their last day.

# 12. Avoiding phishing attacks

Staff will use the following warning signs when considering whether a communication may be unusual:

- Is it from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from a large organisation?
- Is it addressed to a 'valued customer', 'friend' or 'colleague'?
- Does it contain a veiled threat that asks the staff member to act urgently?
- Is it from a senior member of the school asking for a payment?
- Is it from a supplier advising of a change in bank account details for payment?
- Does it sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.
- Is it from a generic email address, such as Gmail or Hotmail?

To prevent anyone having access to unnecessary personal information, the Headteacher will ensure the school's social media accounts and websites are reviewed on a termly basis, making sure that only necessary information is shared. The headteacher will ensure the school's Technology Acceptable Use Agreement for Staff includes expectations for sharing of information and determines what is and is not appropriate to share.

The headteacher will ensure parents, pupils, staff and other members of the school community are aware of acceptable use of social media and the information they share about the school and themselves.

# 13. Training and awareness

The Headteacher will arrange training staff on an annual basis to ensure they are aware of cyber security and how to keep themselves safe online. This will cover identifying irregular

methods of communication in order to help staff members spot requests that are out of the ordinary, such as receiving an invoice for a service not used, and who to contact if they notice anything unusual. Unusual communications could come in a variety of forms, e.g. emails, phone calls, text messages or social media messages.

Staff with access to the school's IT network will be required to undertake basic cyber-security training upon induction which is refreshed every year. At least one member of the governing board will also take part in this training. The training will focus on the following:

- Phishing
- Password security
- Social engineering
- The dangers of removable storage media

All staff 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 Disciplinary Policy and Procedure.

The pupils are taught how to keep themselves safe online through our computing scheme of work. They also participate in Online Safety week each year.

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.

## 14. Potential breaches of security or confidentiality

If staff become aware that information has not been handled according to procedures and there is a data breach or potential security incident, they must report it immediately to **Jeanette Lovejoy (Headteacher) / Lydia Mortimer (SBM)**.

For losses of equipment or if you believe your email or the network may be at risk, contact the **ICT Service Desk** immediately on **01926 414100.**

If equipment or confidential information has been stolen report to the Police and obtain a crime reference number.

Use the school security breeching procedure to report and record incidents. (See Appendix 1).

If you are aware of a potential incident or if you are not sure whether the issue is a security breach then please complete this form as fully as possible and email to: head2410@welearn365.com as soon as possible and in any event within 4 hours.

## 15. Monitoring and review

This policy will be reviewed by the **Headteacher** and the **Governing Body** on an **annual** basis. The next scheduled review date for this plan is **March 2027.**

The Headteacher will be responsible for monitoring the effectiveness of this policy, amending necessary procedures and communicating any changes to staff members.

**Appendix 1**

# Security Breach Reporting Form

| | |
|---|---|
| Name | |
| Date | |
| Time | |
| What has happened? | |
| When and how you found out about the breach? | |
| Signed | |

*To be completed by DPO:*

| | |
|---|---|
| DPO | |
| Date and Time received | |
| Who may have been affected by the breach? | |
| What you are doing as a result of the breach? | |
| Date and time ICO contacted (if necessary)(Within 72 hours) | |
| Signed | |

Appendix 2

# Timeline of Incident Management

| Date | Time | Activity | Decision | Name/position | Date |
|---|---|---|---|---|---|
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |