Padiham Green CE Primary School

Jesus said, "Come Follow Me." Matthew 4:19

Staff Internet Security Policy 2025 - 2026

Review of this Policy: This policy will be reviewed annually by the Governing Board

Revised: September 2025

1. Introduction

Our electronic communications systems and equipment are intended to promote effective communication and working practices throughout the school and are critical to the success of our provision of an excellent service.

This policy outlines the standards that the School requires all users of these systems to observe, the circumstances in which the School will monitor use of these systems and the action the School will take in respect of any breaches of these standards.

The use by staff and monitoring by the School of its electronic communications systems will involve the processing of personal data and is therefore regulated by the General Data Protection Regulation and the Data Protection Act 2018. Staff are referred to the School's Data Protection Policy for further information.

2. Policy Scope

This policy applies to all staff including employees and temporary staff such as agency workers and volunteers. It is to be used in conjunction with the other policies and procedures at Padiham Green CE Primary School and is to be considered like all other staff policies, an extension of the 'Staff Code of Conduct'.

Any employee found to be knowingly in breach of this policy may be subject to the school's disciplinary procedures and review by the headteacher.

3. Equipment security and passwords

All members of staff are responsible for the security of the equipment allocated to or used by them and must not allow it to be used by anyone other than in accordance with this policy. They have a duty to ensure that any networks at 'home' are secure and protect school equipment from cyber attack.

Passwords are unique to each user and must be changed regularly to ensure confidentiality. Staff are required to select a strong password which contains at least 9 characters including both numbers and letters. Passwords which relate to children, pets, or any other information which is easily identifiable (e.g. via social media) should not be used. Passwords should not include the following phrases or words (this is not an exhaustive list):

- Password
- Padiham or Green
- School
- Let me in
- Class
- 123

- Greeners
- PG or Pad

Passwords must be kept confidential and must not be made available to anyone else.. Any member of staff who discloses his or her password to another employee in the absence of express authorisation will be liable to disciplinary action under the School's Disciplinary Policy and Procedure.

Under no circumstances should any staff member log on to a computer using another member of staff's password. Such breaches may result in disciplinary action being taken.

If given access to the School email system or to the internet, staff are responsible for the security of their terminals. Staff are required to log off/lock screen when they are leaving the terminal unattended or when leaving the office to prevent unauthorised users accessing the system in their absence. The Senior Leadership Team may perform spot checks from time to time to ensure compliance with this requirement.

Staff should be aware that if they fail to log off/lock screen and leave their terminals unattended they may be held responsible for another user's activities on their terminal in breach of this policy, the School's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

Logging off/locking screen prevents another member of staff accessing the system in the user's absence and may help demonstrate in the event of a data breach that he or she was not the party responsible.

Staff without authorisation should only be allowed to use terminals under supervision. Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered with.

Members of staff who have been issued with a laptop or tablet must ensure that it is kept secure at all times, especially when travelling (e.g. stored safely in boot of car). Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event that the machine is lost or stolen. Staff should also observe basic safety rules when using such equipment e.g. ensuring that they do not use or display such equipment in isolated or dangerous areas. Staff should also be fully aware that if using equipment on public transport, documents can be easily read by other passengers.

4. Systems use and data security

Members of staff should not delete, destroy or modify any of the School's existing systems, programs, information or data which could have the effect of harming or exposing to risk or harm the School, its staff, pupils, or any other party.

All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the headteacher who will

consider genuine requests for work purposes. Please note that this includes instant messaging programs, screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.

Where consent is given all files and data should always be virus checked before they are downloaded onto the School's systems. If in doubt, the employee should seek advice from the school's ITC Coordinator.

The following must never be accessed from the network because of their potential to overload the system or to introduce viruses:

- audio and video streaming (unless used for educational purposes from a reputable website);
- instant messaging;
- chat rooms;
- social networking sites; and
- personal email (such as Hotmail or Gmail).

No personal devices are permitted to connect to schools WIFI and network, without the prior authorisation of the headteacher. No personal mobile devices are allowed to be connected to school's WIFI at any time.

Staff should not connect any school devices or laptops which connect to school's WIFI/network to any open networks i.e. supermarkets, cafes and large scale conference centres. Where this is necessary for training purposes staff must ensure 'network discovery' is turned off.

The School monitors all emails passing through its systems for viruses. Staff should be cautious when opening emails from unknown external sources or where for any reason an email appears suspicious (such as ending in '.exe'). The headteacher should be informed immediately if a suspected virus is received. The School reserves the right to block access to attachments to email for the purpose of effective use of the system and compliance with this policy. The School also reserves the right not to transmit any email message.

Staff should not attempt to gain access to restricted areas of the network or to any password-protected information unless they are specifically authorised to do so.

Misuse of the School's computer systems may result in disciplinary action up to and including summary dismissal. For further guidance on what constitutes misuse please see the section entitled "Inappropriate Use of the School's Systems" and guidance under "Email etiquette and content" below.

5. Email etiquette and content

Email is a vital business tool, but often lapses inappropriately into an informal means of communication and should therefore be used with care and discipline.

The School's email facility is intended to promote effective communication within the school on matters relating to School's activities and access to the School's email facility is provided for work purposes only.

Staff are not permitted to use school systems for personal use under any circumstances.

School equipment must not be used in school for personal use and can only be used for minimal and in offence personal use outside of school if express authorisation has been granted by the headteacher.

Staff should always consider if email is the appropriate medium for a particular communication. The School encourages all members of staff to make direct contact with individuals rather than communicate by email wherever possible to maintain and enhance good working relationships.

Messages sent on the email system should be written as professionally as a letter or fax message and should be concise and directed only to relevant individuals on a need to know basis. The content and language used in the message must be consistent with the School's best practice.

Emails should never be sent in the heat of the moment or without first checking the content and language and considering how the message is likely to be received. Staff are encouraged wherever practicable to write a draft email first, print it out and review it carefully before finalising and sending. As a rule of thumb if a member of staff would not be happy for the email to be read out in public or subjected to scrutiny then it should not be sent. Copies of emails should be retained on the appropriate file.

Email messages may of course be disclosed in legal proceedings or via a subject access request in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email is obliterated and all email messages should be treated as potentially retrievable, either from the main server or using specialist software. This should be borne in mind when considering whether email is an appropriate forum of communication in the circumstances of the case and if so the content and language used.

Staff should assume that email messages may be read by others and not include in them anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain. The School standard disclaimer should always be used on every email.

Staff should ensure that they access their emails at least once every working day, stay in touch by remote access when travelling or working out of the office and should use an out of office response when away from the office for more than a day. Staff should endeavour to respond to emails marked 'high priority' as soon as is reasonably practicable.

Members of staff are strictly forbidden from sending abusive, obscene, discriminatory, racist, harassing, derogatory or defamatory messages. If such messages are received, they should not be forwarded and should be reported to a member of the Senior Leadership Team immediately. If a recipient asks you to stop sending them personal messages, then always stop immediately. Where appropriate, the sender of the email should be referred to this policy and asked to stop sending such material.

If you feel that you have been harassed or bullied, or are offended by material sent to you by a colleague via email, you should inform the Headteacher who will usually seek to resolve the matter informally in the first instance. You should refer to our Equal Opportunities and Diversity Policy and the Anti-Harassment and Bullying Policy for further information and guidance.

6. Use of the web and the internet

When a website is visited, devices such as cookies, tags or web beacons may be deployed to enable the site owner to identify and monitor visitors. If the website is an inappropriate one such a marker could be a source of embarrassment to the School. Staff may even be committing a criminal offence if, for example, the material is pornographic in nature.

Staff must not therefore access from the School's system any web page or any files (whether documents, images or other) downloaded from the web which, on the broadest meaning of those terms, could be regarded as illegal, offensive, in bad taste or immoral. While content may be legal in the UK it may be in sufficient bad taste to fall within this prohibition.

As a general rule, if any person within the School (whether intending to view the page or not) might be offended by the contents of a page, or if the fact that the School's software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy.

Staff should ensure they are aware of Keeping Children Safe in Education 2025, especially in relation to 'Filtering and Monitoring' and 'Cyber Security' and their responsibility in enforcing this in school. More recently staff should also be aware of changes made to this guidance in relation to the use of 'AI' in admin and planning tasks.

Staff should not under any circumstances use School systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information even in their own time.

Remember also that text, music and other content on the internet are copyright works. Staff should not download or email such content to others unless certain that the owner of such works allows this.

The School's website is intended to convey our core values and excellence in the educational sector. All members of staff are encouraged to give feedback concerning the site and new ideas and inclusions are welcome. All such input should be submitted to the Senior

Leadership Team in the first instance. Only expressly authorised and designated members of staff are permitted to make changes to the website.

Do NOT give school's WIFI password to any visits, supply agency staff, contractors or volunteers without permission from the headteacher after ensuring that the visiting laptop/equipment has sufficient security messages installed to reduce the risk to cyber security. Any visiting IP addresses should be noted and provided to the IT Coordinator.

7. Inappropriate use of equipment and systems

Misuse or abuse of our telephone or email system or inappropriate use of the internet in breach of this policy will be dealt with in accordance with the School's Disciplinary Policy and Procedure.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, any of the following is prohibited:

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading, displaying or disseminating material that is discriminatory, offensive, embarrassing or derogatory;
- transmitting confidential information about the School and any of its staff, pupils or associated third parties – without a reasonable and appropriate reason and without authorisation from the headteacher;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School;
- downloading or disseminating material in breach of copyright;
- copying, downloading, storing or running any software without the express prior authorisation of the Senior Leadership Team.
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with our Disciplinary Policy and Procedure, involving the examination and disclosure of documents, systems and monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

8. Taking Information Off Site

The school allows staff to take children's workbooks off site for the purposes of marking and assessment, where the data does not contain identifiable data markers. These should be treated in the same way as laptops and tablets in that reasonable measures both at home and in transit should be made to keep them safe.

When taking pupils off site for educational visits, it is standard practice to take a hard copy of pupil contact details and health care plans etc. in case of emergency. Owing to the sensitivity of this kind of information, a greater degree of care should be taken to keep the information secure and confidential. For the avoidance of doubt, such information must never be left unattended (unless it is securely locked away) or left in a place where it can be accessed by others. Wherever possible, information should be kept in a lockable bag. On return, the hard copies must be handed back into the school office who will shred them.

There will be occasions when highly sensitive meetings cannot take place within the school building e.g. child protection conferences and strategy meetings. In these instances, it may be necessary to print off hard copies of highly confidential information for the purposes of the meeting. Only the headteacher, deputy headteacher and SENDCO have the automatic right to do this. Information taken off site must be logged and signed off and shredded on return to site.

If other members of staff need to take hard copies of sensitive information out of the building, they must first seek approval from the headteacher and you must ensure that doing so does not breach the school's Data Protection Policy.

9. Monitoring and review

The headteacher and governing board will review this policy on an **annual** basis, making any necessary changes.

The next scheduled review date for this policy is **September 2026**.