

Information Security Policy

Approval: March 2025
Date of March 2026
Review:
Next Review: 1 year / change in legislation

Introduction

1.1 Our electronic communications systems and equipment are intended to promote effective communication and working practices throughout Park Brow Primary School.

1.2 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.

1.3 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 UK General Data Protection Regulation and the Data Protection Act 2018. Staff are referred to the School's Data Protection Policy for further information.

Policy

1. Scope 2.1 This policy applies to all staff including employees and temporary staff such as agency workers. It does not form part of any employee's terms and conditions of employment and is not intended to have contractual effect. It is provided for guidance to all members of staff at the school who are required to familiarise themselves and comply with its contents. The school reserves the right to amend its content at any time. Where reference is made in this policy to a member of staff seeking authorisation from the Head teacher those not working within a school should read this as their line manager.
2. 2.2 References to "equipment" or "devices" means equipment or devices issued by the school as well as any personal equipment or devices that may be used by staff for work purposes.
3. 2.3 References to "information" apply equally to electronic and hard copy information.

1. Equipment security and passwords 3.1 The school operates a 'clear desk' policy which staff are required to comply with at all times. Our schools will enforce this by way of regular desk sweeps and impromptu checks by a member of the Senior Leadership Team.
2. 3.2 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.
3. 3.3 When transporting and storing equipment and information, staff must ensure that it is not exposed to environmental threats and opportunities for unauthorised access, such as being left in an unattended vehicle.
4. 3.4 Staff must ensure that they are in an appropriate location before accessing equipment, devices or information to reduce the risk of unauthorised access.
5. 3.5 Staff must only create hard copies of electronic information where it is absolutely necessary. Hard copies must be:
6. (a) treated in accordance with this policy;

3.6 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 6 characters including both numbers and letters, uppercase and lower case. Passwords which relate to children, pets, or any other information which is easily identifiable (e.g. via social media) should not be used.

3.7 Passwords must be kept confidential and must not be made available to anyone else unless authorised by a member of the SLT.

3.8 Under no circumstances should any staff member log on to a computer using another member of staff's password.

3.9 If given access to the school's 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 SLT may perform spot checks from time to time to ensure compliance with this requirement.

3.10 Staff members must lock and securely store away devices and information when stepping away from the area in which they are working no matter how briefly this period may be. 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 Trust's Data Protection Policy and/or the requirement for confidentiality in respect of certain information.

3.11 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.

3.12 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.

3.13 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.

(b) backed up by way of making an electronic copy saved to the school's systems; and
(c) securely destroyed as soon as it is no longer required to be kept in hard copy in accordance with the school's Retention schedule

Connecting devices to our systems

1. 4.1 No device or equipment should be attached to our systems without the prior approval of SLT. This includes, but is not limited to, any laptop, mobile phone, iPad, telephone, smart watch, USB device, digital camera, MP3 player, infra-red, Bluetooth connection device or any other electronic device.
2. 4.5 You must comply with the School's policies and procedures when connecting any device to our systems.
3. 4.7 The school shall not be responsible for any matters affecting a device that is connected to its systems, whether with or without permission.

Systems use and data security

1. 5.1 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.
2. 5.2 All members of staff are prohibited from downloading, installing or running software from external sources without obtaining prior authorisation from the Head teacher 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.
3. 5.3 Where consent is given all files and data should always be virus checked before they are downloaded onto the Trust's systems. If in doubt, the employee should seek advice from the IT services provider.

5.5 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 SLT 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. For further guidance on viruses and malicious software please see the sections entitled "Malware Protection" and "Avoiding Phishing Attacks" below.

5.6 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.

(e) personal email (such as Hotmail or Gmail).

1. Email etiquette and content

2. 6.1 Email is a vital tool, but often lapses inappropriately into an informal means of communication and should therefore be used with care and discipline.
3. 6.2 The school's email facility is intended to promote effective communication within the school on matters relating to Trust activities and access to the school's email facility is provided for work purposes only.
4. 6.4 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.
5. 6.5 Messages sent on the email system should be written as professionally as a letter 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 Code of Conduct.
6. 6.7 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 form of communication in the circumstances of the case and if so the content and language used.

6.8 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.

Use of the web and the internet

1. 7.1 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.
2. 7.2 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.
3. 7.4 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.

7.5 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.

7.6 The school's websites are 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 SLT in the first instance.

1. Inappropriate use of equipment and systems 9.1 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.
2. 9.2 Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, any of the following is prohibited:

9.4 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.

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

- (a) accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- (b) transmitting a false and/or defamatory statement about any person or organisation;
- (c) sending, receiving, downloading, displaying or disseminating material that is discriminatory, offensive, embarrassing or derogatory;
- (d) transmitting confidential information about the school and any of its staff, pupils or associated third parties;
- (e) transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the Trust);
- (f) downloading or disseminating material in breach of copyright;
- (g) copying, downloading, storing or running any software without the express prior authorisation of the IT Services SLA provider;
- (h) engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- (i) forwarding electronic chain letters and other materials;
- (j) accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Taking information off site

1. 0.1 Information being posted must either be hand delivered or posted by recorded delivery. A record must be kept of the time and place of hand delivery or, in the case of posting, the tracking reference, and the date and time that receipt of the information is confirmed.
2. 10.2 The school allows staff to take children's workbooks off site for the purposes of marking and assessment. 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.
3. 10.3 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.

10.4 There will be occasions when highly sensitive meetings cannot take place within a 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 Head of School, deputy Headteacher, SENCO and Pastoral Leads have the automatic right to do this. Information taken off site must be logged and signed off and shredded on return to site. The same steps as documented in 10.3 should be taken to safeguard the information.

10.5 If other members of staff need to take hard copies of sensitive information out of the building, they must first seek approval of the Head teacher or in their absence the Deputy Head.

10.6 Our schools will keep a document removal record which will track the movements of hard copy documents taken off site. This record will include the following information:

- (a) Type of document;
- (b) Name of staff member who requested to remove document from the school site and purpose of the removal;
- (c) Name of staff member (who must be from the Senior Leadership Team) who approved the removal;
- (d) Location that document is approved to be removed to;
- (e) How the document will be transported;
- (f) Date that the document is returned to the school site.

Malware prevention

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

1. 11.2 The school will ensure that all school devices have secure malware protection and undergo regular malware scans in line with specific requirements. This will be updated in the event of any attacks to the school's hardware and software. Staff should ensure that their devices are updated when prompted at the earliest opportunity.
2. 11.3 The school will deploy mail security technology, which will detect and block any malware that is transmitted by e-mail. This will also detect any spam or other messages which are designed to exploit users. However, staff should be aware that this will not prevent a phishing attack

Avoiding phishing attacks

1. 12.1 Phishing is a type of social engineering where an attacker sends a fraudulent message (usually by e-mail) designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure. The message is often disguised to look like it is from a legitimate source and may ask the recipient to click on a link

which will request username and password information or open a file which will contain malicious software.

12.2 The school will organise regular training for staff members aimed at preventing falling victim to a phishing attack. This will cover identifying irregular e-mails 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.

12.3 Staff should take note of the following warning signs when considering whether an e-mail may be unusual:

12.4 Staff should check the spelling of the sender's e-mail address to see if it matches their official address. Attackers will often simply amend one or two letters which may be difficult to spot without proper care and attention. If in doubt, staff should refrain from clicking on links or opening attachments without first raising their concerns with the IT Department.

- Is the e-mail from overseas?
- Is the spelling, grammar and punctuation poor?
- Is the design and quality what you would expect from the organisation it has purportedly come from?
- Is the e-mail unsolicited and unlinked to a known task or project?
- Is the e-mail addressed to a 'valued customer', 'friend' or 'colleague'?
- Is the e-mail asking the staff member to act urgently?
- Is the e-mail asking for a payment?
- Does the e-mail sound too good to be true? It is unlikely someone will want to give another individual money or access to another service for free.