Acceptable use of ICT, Internet and Communications Systems Policy

Review Due:	**May 2023 **** *Please note that to support a realignment of policies review across the Trust, the Board of Trustees have approved an extension to the review of this policy to July 2023*
Last Review	New Policy – May 2021
Applicable to:	All Trust Schools
Reviewed By:	ZD & JE
Approved By:	Trust Board

Comments:
New policy created to replace information sheet sent to new staff.

Contents

---

1. About this policy

1.1 New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity, and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative, efficient and productive in their work. All users should have an entitlement to safe internet access at all times.

1.2 Our IT and communications systems are intended to promote effective communication, teaching and working practices within The Partnership Trust. This policy outlines the standards that must be observed when using these systems, the circumstances in which use will be monitored, and the action will be taken in respect of breaches of these standards.

1.3 This policy covers all employees, officers, consultants, contractors, volunteers, casual workers, agency workers, supply teachers and TA's and anyone who has access to our IT and communication systems. They should all be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

1.4 Misuse of IT and communications systems can damage The Trust, individual schools in The Trust and our reputation. Staff are referred to the contents of the Staff Code of Conduct. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.5 This policy does not form part of any employee's contract of employment and we may amend it at any time.

2. Personnel responsible for the policy

2.1 The Senior Leadership teams have overall responsibility for the effective operation of this policy and for ensuring compliance with the relevant statutory framework.

2.2 The Senior Leadership Teams have a specific responsibility to ensure the fair application of this policy and all members of staff are responsible for supporting colleagues and ensuring its success.

2.3 The school will deal with requests for permission or assistance under any provisions of this policy, and may specify certain standards of equipment or procedures to ensure security and compatibility.

3. Equipment security and passwords

3.1 You are responsible for the security of the equipment allocated to or used by you, and must not allow it to be used by anyone other than in accordance with this policy.

3.2 You are responsible for the security of any computer end point used by you. You should lock your machine or log off when leaving it unattended, to prevent unauthorised users accessing the system in your absence.

3.3 Desktop PCs and cabling for telephones or computer equipment should not be moved or tampered without approval from your IT support service.

3.4 You should use passwords on all IT equipment, particularly items that you take off site. You must keep your passwords confidential. You must not use another person's username and password or make available or allow anyone else to log on using your username and password unless authorised by the Headteacher or your IT support service. On the termination of employment (for any reason) you must return any equipment, key fobs or cards. Your log in account will be suspended from the day you leave.

3.5 If you have been issued with a laptop, tablet computer, smartphone or other mobile device, you must ensure that it is kept secure at all times, especially when travelling. This includes ensuring that, if it is left in your vehicle unattended, it is kept in a locked boot. Passwords must be used to secure access to data kept on such equipment to ensure that confidential data is protected in the event of loss or theft.

3.6 School devices may be used on public transport, however, they must be kept with you at all times and not left unattended. Equipment should be kept in any casing or covering provided, and be transported with care. You should also be aware that when using equipment away from school, documents may be read by third parties, for example passengers on public transport, and you are responsible for maintaining confidentiality of any information.

3.7 You should not take any confidential data offsite using an external device, or personal cloud based storage, unless the data or device has been encrypted.

3.8 The rules set out in this agreement also apply to the professional use of any school or personal ICT devices.

3.9 If using personal hand held / external devices (PDAs / laptops / mobile phones / USB devices etc) in school, you will follow the rules set out in this agreement, in the same way as if you were using school equipment. You should follow any additional rules set by the school about such use. You will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.

3.10 You will not disable or cause any damage to school equipment, or the equipment belonging to others.

4. Systems and data security

4.1 You must use school ICT systems in a responsible way, to ensure that there is no risk to your safety or to the safety and security of the ICT systems and other users. You should recognise the value of the use of ICT for enhancing learning and ensure that students receive opportunities to gain from the use of ICT. Where possible, you should educate the young people in your care in the safe use of ICT and embed e-safety in your work with young people.

4.2 You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties). You should not access, copy, remove or otherwise alter any other user's files, without their express permission.

4.3 You must not download or install software from external sources without authorisation from the Headteacher or your IT support service. This includes software programs, instant messaging programs, screensavers, photos, video clips and music files. If in doubt, staff should seek advice.

4.4 You must not attach any device or equipment to the system without authorisation from your Headteacher or IT support service. This includes any USB flash drive, MP3 player, tablet, smartphone or other similar device, whether connected via the USB port, or in any other way.

4.5 You should only transport, hold, disclose or share personal information about yourself or others, as outlined in the Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.

4.6 All emails passing through our system are monitored for viruses. You should exercise particular caution when opening unsolicited emails from unknown sources or an email which appears suspicious (for example, if it contains a file where the name ends in .exe). You should only open attachments if the source is known and trusted. Inform the Headteacher or your IT Support Service immediately if you suspect your computer may have a virus or if you have inadvertently downloaded a harmful / unknown programme. We reserve the right to delete or block access to emails or attachments in the interests of security. We also reserve the right not to transmit any email message.

4.7 You should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of your duties.

4.8 You must be particularly vigilant if you use school IT equipment off-site and take such precautions as we may require from time to time against importing viruses or compromising system security. The system contains information which is confidential and / or subject to data protection legislation. Such information must be treated with extreme care.

4.9 You should ensure that your data is regularly backed up, in accordance with relevant school policies.

4.10 Immediately report any damage or faults involving equipment or software, however this may have happened.

4.11 The Data Protection Policy requires that any staff or student data to which you have access, will be kept private and confidential, except when it is deemed necessary that you are required by law or by school policy to disclose such information to an appropriate authority.

4.12 You are responsible for your actions in and out of school and this Acceptable Use Policy applies not only to your work and use of school ICT equipment in school, but also applies to the use of school ICT systems and equipment out of school and your use of personal equipment in school or in situations related to your employment by The Trust.

5. Media

5.1 You will ensure that when you take and / or publish images of others you do so with their permission and in accordance with the school's policy on the use of digital media.

5.2 You will not use any personal equipment to record images or video, unless a written agreement providing specific details has previously been made with the ICT Co-ordinator. If this is the case you should make sure the media is deleted before the device is removed from the school site.

5.3 Where data is published it should not be possible to identify by name, or other personal information, those who are featured.

6. Email

6.1 Although email is a vital communication tool, you should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by email should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals. Our standard disclaimer will always be included by default.

6.2 You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate emails. You should communicate with others in a professional manner, not use aggressive or inappropriate language and appreciate that others may have different opinions. Anyone who feels that they are being or have been harassed or bullied, or is offended by material received from a colleague via email, should inform their line manager or the HR department.

6.3 You should take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract. Remember that you have no control over where your email may be forwarded by the recipient. Avoid saying anything which would cause offence or embarrassment if it was forwarded to colleagues or third parties, or found its way into the public domain.

6.4 Email messages are required to be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable, either from the main server or using specialist software.

6.5 In general, you should not:

(a) send, forward or read private emails at work which you would not want a third party to read;
(b) send or forward chain mail, or junk mail;
(c) agree to terms, enter into contractual commitments or make representations by email unless appropriate authority has been obtained. A name typed at the end of an email is a signature in the same way as a name written at the end of a letter;
(d) download or email text, music or any other content on the internet which is subject to copyright protection, unless it is clear that the owner of such works allows this;
(e) send messages from another person's email address (unless authorised) or under an assumed name;
(f) send confidential messages via email or the internet, or by other means of external communication which are known not to be secure;
(g) communicate with students and parents / carers unless using official school systems. Any such communication should be professional in tone and manner.

6.6 If you receive an email in error you should inform the sender.

6.7 Do not use your own personal email account to send or receive email for work purposes. Only use the email account(s) we have provided for you.

7. Using the internet

7.1 The school ICT systems are primarily intended for educational use and you should only use the systems for personal or recreational use within the rules set out in this policy.

7.2 When a website is visited, devices such as cookies, tags or web beacons may be employed to enable the site owner to identify and monitor visitors. If the website is of a kind described in paragraph 9.1, such a marker could be a source of embarrassment to the visitor and us, especially if inappropriate material has

been accessed, downloaded, stored or forwarded from the website. Such actions may also, in certain circumstances, amount to a criminal offence if, for example, the material is pornographic in nature.

7.3 Any use of social networking sites or participation in internet chat rooms, message boards, blog or wiki should only be used in school where it is required for the proper performance of your duties, or in accordance with sections 9 and 10 of this policy.

7.4 You should not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. Even web content which is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not), might be offended by the contents of a page, or if the fact that our 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. You should not try to use any programs or software that might allow the bypass of the filtering / security systems in place to prevent access to such materials.

7.5 You should not engage in any on-line activity that may compromise your professional responsibilities.

7.6 You should ensure that you have permission to use the original work of others in your own work.

7.7 Alongside this policy you should also read the following policies which can be found on The Trust's website:

- Trusts GDPR Information Security Policy;
- Trusts GDPR Data Protection Policy;
- Trusts Remote Learning Policy.

8. Monitoring

8.1 IT systems within schools enable us to monitor email, internet and other communications. In order to carry out legal obligations in our role as an employer, use of school systems and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for safeguarding purposes.

8.2 We reserve the right to retrieve the contents of email messages or to check internet usage (including pages visited and searches made) as reasonably necessary in the interests of safeguarding and monitoring, including for the following purposes (this list is not exhaustive):

(a) to monitor whether use of the email system or the internet is legitimate and in accordance with this policy;
(b) to find lost messages or to retrieve messages lost due to computer failure;
(c) to assist in the investigation of alleged wrongdoing;
(d) to comply with any legal obligation.

9. Prohibited use of our systems

9.1 Misuse or excessive personal use of our telephone or email system or inappropriate internet use will be dealt with under the Trust Disciplinary Procedure. Misuse of the internet can in some circumstances be a criminal offence. Examples of misuse include participating in online gambling, forwarding chain letters, or by creating, viewing, accessing, transmitting or downloading any of the following material (this list is not exhaustive):

(a) pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);
(b) offensive, obscene, or criminal material or material which is liable to cause embarrassment to us or to our clients or customers;
(c) a false and defamatory statement about any person or organisation;

(d) material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);
(e) confidential information about us, The Trust and schools within The Trust, or any of our staff, students or educational colleagues (except as authorised in the proper performance of your duties);
(f) unauthorised software;
(g) any other statement which is likely to create any criminal or civil liability (for you or us);
(h) music or video files or other material in breach of copyright;
(i) material pertaining to the planning of malicious, violent or controversial acts.

9.2 Where evidence of misuse is found, we may undertake a more detailed investigation in accordance with our Disciplinary Procedure, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Procedure. If necessary, such information may be handed to the police in connection with a criminal investigation.

9.3 You will immediately report any illegal, inappropriate or harmful material or incident you become aware of, to the Headteacher or IT support Service.

9.4 Use of the systems or equipment to access or create content which could be embarrassing to The Trust or that could bring The Trust into disrepute is considered as misuse.

9.5 The content of storage areas supplied by the school (document storage areas / mailbox / OneDrive / shared storage area / personal storage area) is for the purpose of storing content in relation to the proper performance of your duties. The school systems and devices are not to be used for any kind of malicious or controversial planning of material, or to store such items. The Trust reserves the right to monitor storage areas and disclose any such findings as appropriate, in accordance with this policy.

10. Personal use of our systems

10.1 We permit the incidental use of our internet, email and telephone systems to send personal email, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

10.2 Personal use must meet the following conditions:

(a) use must be minimal and take place substantially out of normal working hours (that is, during lunch hours, before 8:30 am or after 4:30 pm);
(b) use must not interfere with business or office commitments;
(c) use must not commit us to any marginal costs;
(d) use must comply with this policy.

10.3 We reserve the right to restrict or prevent access to certain telephone numbers, internet sites or applications if we consider personal use to be excessive.

End of policy