PDET

Acceptable Use Policy

(ICT and Internet)

Date	Revision & Amendment Details	By Whom
July 2023	Revisions to the policy approved (bar appendices)	Business & Finance Committee

CONTENTS

1. Introduction and Aims

Information and communications technology (ICT) is an integral part of the way Peterborough Diocese Education Trust ('The Trust') works, and is a critical resource for pupils, staff, directors, governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the Trust and its schools.

However, the ICT resources and facilities the Trust and its schools use could also pose risks in relation to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of Trust / school ICT resources and personal devices used for Trust / school business
- Establish clear expectations for the way all members of the Trust / school community engage with each other online
- Support the Trust's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the Trust / schools through the misuse, or attempted misuse, of ICT systems
- Support the schools in teaching pupils safe and effective internet and ICT use.

  This policy covers all users of the Trust / schools' ICT facilities and those users who use personal devices for school / Trust business, including directors, central team members, governors, staff, pupils, volunteers and visitors.

2. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- *Data Protection Act 2018*
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by *The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020*
- *Computer Misuse Act 1990*
- *Human Rights Act 1998*
- *The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000*
- *Education Act 2011*
- *Freedom of Information Act 2000*
- *Education and Inspections Act 2006*
- Latest edition of *Keeping Children Safe in Education*
- *Searching, screening and confiscation: advice for schools 2022*
- *National Cyber Security Centre (NCSC): Cyber Security for Schools*
- *Education and Training (Welfare of Children) Act 2021*
- UKCIS guidance on *sharing nudes and semi-nudes: advice for education settings working with children and young people*
- *Meeting digital and technology standards in schools and colleges*.

3. Related Policies

This policy should be read alongside the Trust / school's policies on:

- *IT Controls*
- *Cyber Response Plan*
- *Safeguarding / Child Protection*
- *Staff Code of Conduct*
- *Data protection and Information Rights*
- *Remote Education: Online safety (Safeguarding and GDPR considerations) Guidance for schools / academies*
- *Remote Education: Guidelines For Parents / Carers and Pupils.*

4. Definitions

ICT facilities: all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the Trust / school's ICT service.

Authorised users (users): anyone authorised by the Trust / school to use the Trust / school's ICT facilities, including directors, governors, staff, central team members, volunteers and visitors or to set up personal devices to access Trust / school business.

Personal use: any use or activity not directly related to the users' employment, study or purpose agreed by Authorised Personnel.

Authorised personnel: employees authorised by the Trust / school to perform systems administration and/or monitoring of the ICT facilities.

Materials: files and data created using the Trust / school's ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

5. Unacceptable Use

The following is considered unacceptable use of the Trust / school's ICT facilities (including when carrying out Trust / school business using personal devices).

Unacceptable use of the Trust / school's ICT facilities includes:

- Using ICT facilities to breach intellectual property rights or copyright
- Using ICT facilities to bully or harass someone, or to promote unlawful discrimination
- Using ICT facilities in a manner that breaches the Trust / school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Using ICT facilities for online gambling, inappropriate advertising, phishing and / or financial scams
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful
- Consensual and non-consensual sharing of nude and semi-nude images and / or videos and / or livestreams

- Activity which defames or disparages the Trust / school, or risks bringing the Trust / school into disrepute
- Sharing confidential information about the Trust/school, its pupils, or other members of the Trust / school community inappropriately
- Connecting any device to the Trust / school's ICT network without approval from Authorised Personnel
- Setting up any software, applications or web services on the Trust / school's network without approval by Authorised Personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the Trust / school's ICT facilities, accounts or data, gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from Authorised Personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the ICT facilities
- Causing intentional damage to the ICT facilities
- Removing, deleting or disposing of the Trust / school's ICT equipment, systems, programs or information without permission from Authorised Personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by Authorised Personnel to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust / school
- Using websites or mechanisms to bypass the Trust / school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. In relation to a school, the Headteacher (or equivalent) will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of ICT facilities.

The Chief Operating Officer (COO) will determine whether any act or behaviour not on the list above is considered unacceptable use of Central Office facilities.

In the event of the unacceptable use being by the Headteacher (or equivalent) or by the COO, the CEO will determine whether any act or behaviour not on the list above is considered unacceptable use. In the event of unacceptable use by the CEO, the Chair of Directors will make such determination.

5.1 Exceptions from Unacceptable Use

Where the use of ICT facilities (on school premises/ at the Central office and / or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's, COO's or CEO's discretion, as appropriate.

In the event of a Headteacher / COO granting an exemption, they will document the reasons and send this to the COO / CEO, as appropriate, preferably in advance of the activity. The COO / CEO, as appropriate will record the exemption.

5.2 Breach of this Policy

It is each staff member's responsibility to ensure the contents of this policy have been read and fully understood and to ensure it is effectively put into place where relevant to each staff member's own duties and responsibilities.

In addition to any training received from the Trust (such as CyberEssentials) staff should also work with their line manager to ensure CPD and / or training plans contain any relevant aspects needed to ensure awareness and confidence in using digital resources and technology devices is sufficient for an individual's role and for compliance with this policy.

Any breach of this policy will be taken seriously and may result in disciplinary action in line with the *Trust's Staff Code of Conduct and the Trust's Disciplinary Policy.*

A member of staff who deliberately or recklessly uses or abuses any of the IT facilities provided by the Trust without proper authority may also be guilty of a criminal offence and / or gross misconduct. This may result in dismissal.

6. Staff (including directors, central team members, governors)

6.1 Access to ICT Facilities and Materials

The Trust's Managed Service Provider, Computeam Limited, manages access to ICT facilities. This includes, but is not limited to:

- Computers, tablets, mobile phones and other devices
- Access permissions for certain programs or files.

All users of the ICT facilities will have clearly defined access rights to Trust/school systems, files and devices. Users will be provided with unique login / account information and passwords that they must use when accessing ICT facilities.

Users who have access to content or digital resources that they are not authorised to view or edit, or are able to manipulate Trust data in any way which might constitute a breach of this policy or bypass the controls implemented by the solutions put in place, should immediately report this to the COO and raise a support call with the Computeam Helpdesk on 0800 862 0123.

Users who need their access permissions updated or changed, should contact the Computeam Helpdesk:

- Email: support@computeam.co.uk
- Telephone: 0800 862 0123

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.

7. Using IT Systems and Devices

The Trust is responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff and learners. It therefore takes steps to protect the security of its computing resources, data and user accounts. The effectiveness of these procedures is reviewed periodically to keep up with evolving cyber crime technologies. (*See Trust Cyber Response Plan and IT Controls Policy.)*

Maximum usage of the Trust's Microsoft 365 environment should be made for all communication and collaboration. For additional security, the use of this environment will require provision of second level of authentication every 30 days. This will be in the form of a six-digit code provided via the Microsoft Authenticator app.

A high number of incidents relating to non-controlled use of ICT result from basic, avoidable mistakes being made when using ICT devices and systems. Users should ensure compliance with the following:

7.1 Passwords

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

A password, and any other accompanying security credentials issued, must be kept secure and confidential and must not be shared with, or given to, anyone else. When logging into Trust and school IT systems, a user's own login credentials and password should be used.

All users of the ICT facilities should set strong passwords for their accounts and keep these passwords secure. Passwords should:

- Be at least **eight** characters long
- Contain a mixture of letters, numbers, upper and lower case, and special characters (where accepted)
- Not be so complex that it is difficult to remember without writing it down
- Never be written down
- Be difficult to guess. Information which other people might know, or be able to find out, such as personal addresses or birthdays should not be used.

A password which is used for another account should not be used.

Where temporary passwords are issued to any individual, for any reason, they should be changed at first logon to a permanent password.

Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there could otherwise be a possible compromise of the system. Passwords should not be re-used or recycled across different systems. In accordance with current and recommended best practice within Microsoft Office 365, passwords **will not** expire automatically, the use of additional authentication will keep the account protected.

Failure to comply with these password requirements could lead to compromising system security and would be considered a breach of this policy.

7.2 Locking Computer Screens

Computer screens should be locked when they are not in use / unattended, even if users are only away from the computer for a short period of time. To lock computer screens users should press Ctrl-Alt-Delete (for Windows devices) or press the power / lock button (for tablet devices). If users are not sure how to do this then the ICT helpdesk should be called or the relevant ICT technician

should be contacted. Some devices are configured to automatically lock if not used for a period of time but this should not be relied upon.

7.3 Familiarisation with IT Systems and Devices

Users should ensure that they have familiarised themselves with any software or hardware that is used. In particular, users should make sure that they understand what the software is supposed to be used for and any risks associated. For example:

7.3.1 If virtual / digital resources are used which allow the upload of lesson plans and assessments for pupils, care must be taken that accidental upload of any other information does not occur

7.3.2 Ensure that proper use of any security features contained in software and applications takes place. For example, some software will allow information to be redacted from documents (i.e. "black out" text so that it cannot be read by the recipient). Users should make sure, in this example, that the software is used correctly so that the recipient of the document cannot "undo" the redactions

7.3.3 Extra care needs to be taken where storing information containing Special Category Data. For example, safeguarding information should not ordinarily be saved on a shared computer drive accessible to all staff. If in doubt, the Data Protection Officer should be contacted.

7.4 Hardware and Software provided by the Trust

Users must not use, download or install any software, app, programme, or service without permission from the Trust. Users must not connect (whether physically or by using another method such as Wi-Fi or Bluetooth) any device or hardware to the Trust or school ICT systems without permission.

If users wish to request the installation of a piece of software or app onto a computer, tablet, or mobile device they must first log a support call with the Computeam Helpdesk on 0800 862 0123. Computeam will be able to advise whether the software / app is on the Trust's pre-approved list for installation or whether an additional approval process will be required (if not a pre-approved piece of software / app). The list of pre-approved software and apps is included in *Appendix 1 of the IT Controls Polic*y and will be reviewed and updated regularly as requests are received.

All the Trust's ICT devices that support software updates, security updates and anti-virus products will have these installed and will be configured to perform such updates regularly or automatically. Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards implemented and maintained to protect data and the ICT facilities.

7.5 Private Cloud Storage

Users must not use personal or private cloud storage (e.g. Google Drive, OneDrive) or any external, non-Trust approved file sharing accounts to store or share documents. The shared storage and messaging facilities within Microsoft 365 (SharePoint, Outlook, and Teams) are the only approved methods for storing and / or sharing all data, documents, and other information related to central Trust activities as well as for all management and administrative activities for individual schools. Where Google services are in use these must be limited to classroom (teacher / pupil) activities only. The use of any third-party sharing applications (such as Dropbox, WeTransfer, or equivalents) for the storing or sharing of any Trust or school related data and content is strictly prohibited.

7.6 Portable Media Devices

The use of portable media devices (such as USB drives, portable hard drives, DVDs) is not allowed unless those devices are encrypted and have been supplied by the Trust and training has been received on how to use such devices securely. The ICT support team can protect any portable media device provided, with encryption. However, the use of these should only be in essential or exceptional circumstances with advance approval from the Trust.

7.7 School Phones

School phones must not be used for personal matters. School staff members who are provided with work mobile phones must not do anything which would be deemed as unacceptable use as set out in *section 5*.

7.8 Disposal of Trust IT Equipment

Trust IT equipment (this includes laptops, printers, phones, and any storage media) must always be returned to the ICT support team for disposal even if it is presumed that it is broken and will no longer work. These can then be safely destroyed and data removed securely.

7.9 Use of Email

The Trust / school provides each member of staff (including directors and governors) with an email address and this email account should be used for work purposes only.

Users must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

7.9.1 Private Email Addresses

Private email addresses must not be used for Trust related work; @pdet.org.uk addresses should only be used.

Staff members must not share their personal email addresses with parents / carers and pupils and must not send any work-related materials to parents / carers / pupils using their personal email account.

Directors will be required to use a PDET email address to correspond on applicable matters with staff. For the majority of Board matters (being informed about meetings and document packs), directors are presently permitted to use personal email addresses to access *'Governor Hub'* which holds the information presented. Should a decision be taken to override this permission then directors will be informed separately.

7.9.2 Email Encryption – Special Category Data

Internal and external emails which contain Special Category Data (as defined under the Data Protection Policy) should be encrypted. The Trust uses Egress for sensitive emails which encrypts data including emails whilst at rest and in transit e.g. when sending details of a safeguarding incident to social services. If this additional level of encryption is required, users should contact the Trust central team to obtain guidance on how to do this.

7.9.3 Document Encryption – Special Category Data

Confidential documents containing Special Category Data (as defined under the Trust's *Data Protection Policy*) should be further encrypted by using password protection when attaching to

emails. If a "password" or "key" to unlock an encrypted document needs to be provided, then this should be provided via a different means e.g. a call to the recipient. Any queries about encryption, for example, uncertainty regarding how or when to use it, should be raised with the IT Helpdesk or on-site IT Technicians.

Users must 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. Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.

7.9.4 Sending / Receiving Emails in Error

If users receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they must inform the Trust Operations Manager and the Data Protection Officer, in accordance with the Trust's *personal data breach reporting procedure.*

7.9.5 Emails to Multiple Recipients

Care should be taken when setting up and managing email groups. The IT Helpdesk or on-site IT Technicians can provide advice for ways of communicating to multiple recipients in a secure manner. If an email contains Special Category Data (as defined under the Data Protection Policy) another member of staff should double check that the email address has been entered correctly before pressing send.

7.9.6 Email Auto Forward

Auto forward should not be used in any circumstance on an email account, either internal or external to the Trust, without the approval of the Data Protection Officer and the Trust COO.

7.10 Remote Access / Working Off-Site

Users are permitted to access the ICT facilities and materials remotely as the Trust operates a Single Tenancy in Microsoft Office 365. The tenancy is configured in accordance with the Trust's IT Controls Policy.

Users accessing the ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on site. Users must be particularly vigilant if they use the ICT facilities outside the Trust / school premises and take precautions to limit the risks of importing viruses or compromising system security.

Users should not use public Wi-Fi to connect to the internet. For example, if working in a café, users would need to work offline or tether (hotspot) to the user's mobile phone.

The ICT facilities contain information which is confidential and / or subject to data protection legislation. Such information must be treated with extreme care and in accordance with the Trust's Data Protection Policy.

Whilst travelling, users must not work on documents containing Personal Data if there is a risk of unauthorised disclosure (for example, if there is a risk that someone else will be able to see such information).

If users need to book out a school device for working away from site, this needs to be arranged and authorised by the Headteacher.

7.11 Use of Personal Devices

Staff may only use personal devices (including computers and phones) for work purposes including to access Trust / school data, work remotely, or take personal data (such as pupil information, staff information) out of the Trust premises / school if:

- Specific authorisation has been given by the Headteacher or COO, as appropriate

or

- When required to ensure the safety and security of Trust data and information (i.e. using the Company Portal and Microsoft Authenticator app on a phone to provide a second piece of authentication data when accessing Trust services).

7.11.1 Data Security - Set Up

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption. A number of Microsoft apps should be installed (such as "Authenticator" and "Company Portal") which are required to protect Trust data, and to manage Trust applications and access on your device (often referred to as "Mobile Application Management" or "MAM").

If permission is gained to use a personal laptop or PC for school or Trust work, the ICT support team will prepare the device. This will ensure that Personal Data is only accessed through the Trust's networks and systems, which is more secure and significantly reduces the risk of an Information Security breach.

Appropriate security measures should always be taken. This includes the use of firewalls and anti-virus software. Any software or operating system on the device should be kept up to date. **It is the responsibility of the device owner to ensure the device is kept up to date with the latest operating system, patches, and any security updates.**

No actions should be taken which could prevent any software installed on the personal computer or device by the Trust from working properly. For example, the software should not be uninstalled, or school related documents or data should not be saved to an area of the device that is not protected.

If the personal device came with a default password, then this password should be changed immediately. (See *Section 7.1* of this document for guidance on choosing a strong password.)

Personal devices should not be configured in a way that would allow someone else to access school or Trust related documents and information.

7.11.2 Data Security – Personal Data

Documents containing Personal Data (including photographs and videos) should not be sent to or saved to personal devices unless express permission has been given. This is because anything saved to the personal device will not be protected by the Trust's security systems. Furthermore, it is often

very difficult to delete something which has been saved to a computer. For example, if a school document has been saved to a personal laptop to facilitate work on it over the weekend, the document would still be on the computer hard drive even if deleted and the recycle bin emptied.

7.11.3 Data Security – End Use

If the personal device is no longer used for school or Trust work then all school and Trust information, documents, data (including emails), and any software applications provided by the Trust, must be removed from the device. If this cannot be achieved remotely, the user will be informed by the Trust. Following this, the device must be submitted for wiping and software removal. All necessary co-operation and assistance by the user in relation to this process must be provided.

7.11.4 Use of Personal Mobile Phones

Use of a personal mobile phone for day-to-day work activities is strongly discouraged. If you must use a personal mobile, emails must only be accessed by the Outlook app. If the mobile phone is lost or stolen, this could constitute a data breach and the Data Protection Officer should be immediately notified.

School staff members must not give to or use their personal phone number(s) to communicate with parents / carers or pupils - *see Staff Code of Conduct*.

7.12 Personal Use of Trust / School ICT Facilities

Staff are permitted to occasionally use ICT facilities for personal use, subject to certain conditions set out below. This permission must not be overused or abused. The Trust may withdraw or restrict this permission at any time and at their discretion.

Personal use is permitted provided that such use:

- Does not constitute 'unacceptable use', as defined in *section 5*
- Does not interfere with an individual's role, or prevent other users from using the facilities for work or educational purposes
- Does not take place during teaching time
- Takes place when no pupils are present.

Staff may not use the ICT facilities to store personal, non-work-related information or materials (such as music, videos or photos).

Staff should be aware that use of the ICT facilities for personal use may put personal communications within the scope of the school's / Trust / ICT monitoring activities.

7.13 Trust / School Social Media Accounts and Personal Social Media Accounts

The Trust has an official Twitter account, managed by the Central Operations team. Individual schools are authorised to have official social media accounts (Twitter, Facebook, Instagram etc).

Users who have not been authorised to manage, or post to, the account, must not access, or attempt to access, such accounts.

Users should make sure their use of social media, either for work or personal purposes, is appropriate at all times. Users should take care to protect themselves online and avoid compromising their professional integrity.

Users should be aware that personal use of ICT (even when not using Trust / school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents / carers may access them.

Guidelines for staff on appropriate security settings for social media accounts are set out in *Appendix 1*.

7.14 Monitoring and Filtering of the Trust / School Network and Use of ICT Facilities

The Trust's wireless internet connections are secure. All connections are obtained from an education services provider and the Trust ensures that it/each school has appropriate filtering in place.

The Trust / school monitors ICT use in order to:

- Safeguard children
- Obtain information related to Trust / school business
- Investigate compliance with Trust / school policies, procedures and standards
- Ensure effective Trust / school ICT operations
- Conduct training or quality control exercises
- Prevent or detect crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the Trust reserves the right to filter and monitor the use of its ICT facilities and network. This includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited
- Bandwidth usage
- Email accounts
- Telephone calls
- User activity / access logs
- Any other electronic communications.

Where appropriate, Authorised Personnel may raise concerns about monitored activity with the Trust's / school's designated safeguarding lead (DSL), as appropriate.

Only authorised staff may filter, inspect, monitor, intercept, assess, record and disclose the above and only to the extent permitted by law.

The COO will regularly review the effectiveness of school's monitoring and filtering systems.

If, for any reason, content has been accessed which is believed, or known, to be inappropriate this should be brought to the immediate attention of the Designated Safeguarding Lead / Headteacher as appropriate so that the relevant actions can be taken in accordance with the Trust's Safeguarding Policy.

8. Parents / Carers and Visitors

8.1 Access to ICT Facilities and Materials

ICT Facilities: Parents / carers and visitors do not have access to the ICT facilities as a matter of course. However, parents / carers working for, or with, the Trust in an official capacity (for instance, as a staff member) may be granted an appropriate level of access, or be permitted to use the school's facilities at the Headteacher's discretion. Where parents / carers are granted access in this way, they must abide by this policy as it applies to staff.

Internet Access: Parents / carers and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher. The Headteacher will only grant authorisation if:

- Parents / carers are working with the school in an official capacity (e.g. as a teacher or as a member of the parents' association)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan).

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. It is strongly recommended that parents / carers and visitors only have access using a 'Guest' Wi-Fi connection.

Visitors to the Trust central office will only be granted access to the Guest Wi-Fi connection.

8.2 Communicating with or about the School Online

It is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online. Parents / carers play a vital role in helping model this behaviour for their children, especially when communicating with the school through the school's website and social media channels.

Parents / carers are asked to sign the agreement in *appendix 2* and the school's Pupil Acceptable Use Agreement.

Parents / carers may seek any support and advice from the school to ensure a safe online environment is established for their child.

8.3 Communicating with Parents / Carers about Pupil Activity

Schools will:

- Ensure that parents / carers are made aware of any online activity that their children are being asked to carry out
- Communicate the details to parents / carers when pupils are asked to use websites or engage in online activity.

In particular, staff will let parents / carers know which (if any) person or people from the school, pupils will be interacting with online, including the purpose of the interaction.

9. Pupils

9.1 Access to ICT Facilities

Pupils have access to a range of ICT equipment, including but not limited to, laptops and tablets. The following rules apply to pupils when using Trust / school equipment:

- School's computers and specialist ICT equipment are available to pupils only under the supervision of staff
- Pupils will be provided with an account linked to the school's virtual learning environment, which they can access from any device registered with the Trust.

Pupils have to sign the school's Pupils' Acceptable Use Agreement.

9.2 Unacceptable Use of ICT and the Internet

A school will sanction pupils, in line with the Trust Behaviour Policy, if a pupil engages in any of the following during school time and / or using school IT facilities:

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's and / or school's policies or procedures
- Any illegal conduct, or making statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual or non-consensual sharing of nude and semi-nude images and / or videos and / or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password-protected information, without approval from Authorised Personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) authorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and / or those they share it with are not supposed to have access, or without authorisation
- Using inappropriate or offensive language.

If it is brought to the attention of the school that a pupil may have engaged in any of the above outside school hours and / or on personal devices, the school will inform the relevant parties and / or take the appropriate actions. This includes sanctioning a pupil, in line with the Trust Behaviour Policy, if appropriate.

10. Monitoring and Review

The COO monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust and each school.

This policy will be reviewed every three years.

The Directors are responsible for reviewing and determining this policy.

Appendix 1 – Social Media Help Sheet for School Staff

Do not accept friend requests from pupils on social media

10 Rules for School Staff on Social Media

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if you don't, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, your school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling social media apps from your phone. Apps recognise WiFi connections and makes friend suggestions based on who else uses the same WiFi connection (such as parents / carers or pupils).

Check your Privacy Settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**: your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender.

What to do if …

A Pupil adds you on Social Media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and / or their parents / carers. If the pupil persists, take a screenshot of their request and any accompanying messages

- Notify the senior leadership team or the headteacher about what's happening.

A Parent / Carer adds you on Social Media

- It is at your discretion whether to respond. Bear in mind that:
  - Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
  - Pupils may then have indirect access through their parent's / carer's account to anything you post, share, comment on or are tagged in
- If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so.

You're being Harassed on Social Media, or Somebody is Spreading Something Offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, the Trust's mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent/carer or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police.

Appendix 2 - Acceptable Use of the Internet: Agreement for Parents and Carers

Acceptable Use of the Internet: Agreement for Parents and Carers	
Name of parent / carer: **Name of child:**	
Online channels are an important way for parents / carers to communicate with, or about, our school. The school uses the following channels: *Each school to update* • *Our official Facebook page* • *Email / text groups for parents / carers (for school announcements and information)* • *Our virtual learning platform e.g. Microsoft Office 365*	
When communicating with the school via official communication channels, or using private / independent channels to talk about the school, I will: • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents / carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure. I will not: • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues unless they are raised in an appropriate way • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I have a concern about a specific behaviour issue or incident • Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents / carers.	
Signed:	**Date:**

Appendix 3 - Acceptable Use Agreement for Adult Users

Acceptable Use of the Trust / School's ICT Facilities and the Internet: Agreement for Adult Users	
Name of adult:	
When using the Trust / school's ICT facilities and accessing the internet in the Central office / school, or outside these premises on a work device, I will not: • Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material) • Use them in any way which could harm the Trust's / school's reputation • Access social networking sites or chat rooms • Use any improper language when communicating online, including in emails or other messaging services • Install any unauthorised software, or connect unauthorised hardware or devices to the Trust's / school's network • Share my password with others or log in to the Trust / school's network using someone else's details • Share confidential information about the Trust, school, its pupils or staff, or other members of the community • Access, modify or share data I'm not authorised to access, modify or share • Promote private businesses, unless that business is directly related to the Trust / school.	
I understand that the Trust / school will monitor the websites I visit and my use of the Trust / school's ICT facilities and systems. • I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Trust / school premises, and keep all data securely stored in accordance with this policy and the Trust's data protection policy • I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material • I will always use the Trust / school's ICT systems and internet responsibly, and ensure that pupils in my care do so too. I have read and agree to abide by the terms of the Acceptable Use Policy (AUP).	
Signed:	**Date:**

Appendix 4: Device Receipt

Device Receipt

I confirm that I have received the below device(s) and I have read and agreed to the PDET ICT acceptable use policy.

Device Description:

Model Serial Number:

Name: _____

Sign: _____

Date: _____