PONTEFRACT
ACADEMIES TRUST

Acceptable Use Policy

Summary:

This policy sets guidelines and rules on the use of ICT resources for staff, pupils, parents, and governors across the Trust.

Author	Head of Governance		
Applies to: (please check as appropriate)	Staff ☑	Pupil ☑	Community ☑
Ratifying Committee(s):	Education and Standards Committee		
Available on:	Compliance Library ☑	Website ☑	
Date of Approval:	11/10/2023		
Date of Next Formal Review: (ensure this is aligned to committee meeting dates)	11/10/2024		
Review Period:	Annual		
Status:	Non-contractual		
Owner:	**Pontefract Academies Trust**		
Version:	02		

Document Control

Date	Version	Action	Amendments
August 2022	01	New policy	
Sept 2023	02	Reviewed	• References to Director of Operations removed. • Added 'Governance Code of Conduct to Section1, Para.5. • Added homophobic and transphobic to last point of bulleted list of

			unacceptable use descriptors, Section 4, Para. 2. • Added Governance Code of Conduct or Behaviour Policy to the exceptions to unacceptable use, Section 4, Para. 4. • Added ‘Any such material may form part of a Subject Access Request, may be used as evidence in relation to a Complaint, Suspension/Exclusion Panel, Employment Trubunal or any other relevant statutory process of legal proceedings’ to Section 5, Para. 8 • Added ‘Filtering and monitoring, compliant with the requirements of Keeping Children Safe in Education DfE Statutory guidance is in operation with the Trust. The reports generated as a result of filtering and monitoring activities are only accessible to authorized users’ to Section 5, Para. 34. • Added ‘making use of multi-factor authentication settings wherever possible’ to Section 8, Para. 2. • Added Section 8, Para, 14, ‘Particular care should be taken around using systems in the classroom environment or other public areas, with ‘presenter mode’ settings used for any system that contains personal or sensitive information to avoid a data breach occurring and to actively protect the confidentiality of information held by the Trust or school’. • Added ‘or via the Cloud’ to Section 9, Para. 3, bullet point 4. • Added ‘Cyber Security’ to Section 12, Para. 1.

Contents

1. Introduction and aims

Information and communication technology (ICT) is an integral part of the way Pontefract Academies Trust works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors.

However, the ICT resources and facilities across the Trust also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of ICT resources for staff, pupils, parents and governors across the Trust,
- Establish clear expectations for the way all members of the community engage with each other online,
- Support the Trust policy on data protection, online safety and safeguarding,
- Prevent disruption to 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's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under the following policies:

- Disciplinary policy,
- Behaviour & relationships policies,
- Staff code of conduct
- Governance Code of Conduct

2. Relevant legislation and guidance

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

- Data Protection Act 2018
- The General Data Protection Regulation
- 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
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

3. Definitions

- **ICT facilities:** includes 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 ICT service.

- **Users:** anyone authorised by the Trust or school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

- **Personal use:** any use or activity not directly related to the users' employment, study or other relevant purpose.

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

- **Materials:** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed media, web pages, social networking sites and blogs and any content thereof.

See Appendix 3 for a glossary of cyber security terminology.

4. Unacceptable use

The following is considered unacceptable use of the Trust's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust's ICT facilities includes:

- Using the Trust's ICT facilities to breach intellectual property rights or copyright.
- Using the Trust's ICT facilities to bully or harass someone else, or to promote unlawful discrimination.
- Using the Trust's ICT facilities to breach any Trust or school policy or procedure.
- Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- Using the Trust's ICT facilities to access 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 (also known as 'sexting' or youth-produced sexual imagery).
- Activity which defames or disparages the Trust or school, or otherwise risks bringing the Trust school into disrepute.
- Sharing confidential information about the Trust or school, its pupils, or other members of the school community.
- Connecting any device to the school's ICT network without prior approval from authorised personnel.
- Setting up any software, applications or web services on the 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 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 school's ICT facilities.
- Causing intentional damage to ICT facilities.
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation.
- Using inappropriate or offensive language.
- Promoting a private business, unless that business is directly related to the work of the Trust or school.
- Using websites or mechanisms to bypass the school's filtering and monitoring mechanisms.
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic, homophobic, transphobic or discriminatory in any other way.

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Head of Governance and Headteachers will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust's ICT facilities.

Exceptions from unacceptable use

Where the use of Trust ICT facilities (on the school premises 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 Head of Governance's discretion. An email should be sent to the Head of Governance outlining what is required, by whom and for what purpose to allow them to evaluate the risk and determine if authorisation will/will not be provided. Only upon receipt of approval from the Head of Governance can the exception be progressed. If approval is declined, the individual should not progress. If the decline is ignored, the individual will be dealt with under the Disciplinary Policy, Governance Code of Conduct, or Behaviour Policy.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on behaviour/discipline/staff discipline/staff code of conduct/etc.

5. Staff (including governors, volunteers and contractors)

Access to school ICT facilities and materials

The Trust's Executive Leadership Team manages access to the Trust's ICT facilities and materials for staff, with advice from the Head of Governance. That includes, but is not limited to:

- Computers, tablets, mobile phones and other devices,
- Access permissions for programmes and/or files.

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the external ICT service provider.

Use of phones and email

The Trust provides each employee with an email address.

This email account should be used for work purposes only. Employees should enable multi-factor authentication on their email accounts.

All work-related business should be conducted using the email address provided by the Trust.

Employees must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

Employees 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. Any such material may form part of a Subject Access Request, may be used as evidence in relation to a Complaint, Suspension/Exclusion Panel, Employment Trubunal or any other relevant statutory process of legal proceedings.

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.

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

If employees 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 Head of Governance immediately and follow our data breach procedure, as set out in the Information Policy.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher or Head of Governance may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time/teaching hours/non-break time.
- Does not constitute ‘unacceptable use’, as defined in section 4.
- Takes place when no pupils are present.
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes.

Staff may not use the school’s 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 school’s ICT facilities for personal use may put personal communications within the scope of the school’s ICT filtering and monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff are also permitted to use their personal devices (such as mobile phones or tablets) in line with the below:

- All telephones provided are for work related calls.
- Phone calls of a personal nature should be kept brief and restricted to matters of importance.
- Phone calls to international and premium rate numbers are unacceptable at all times, unless specifically required for your professional duties.
- Mobile telephones should be secured with a suitable PIN or Passcode.

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

Staff should take care to follow the Trust’s guidelines on social media (see appendix 1) and use of email (see section 5.1) to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

The school has guidelines for staff on appropriate security settings for Facebook accounts (see appendix 1).

Remote access

We allow staff to access the school’s ICT facilities and materials remotely. They should dial in using a virtual private network (VPN) or via the Cloud, dependent upon the individual setting.

The Cloud service is automatically applied where available. VPN services are provided by the ICT partner and can be requested via the headteacher, where necessary.

Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as advised by the headteacher, Head of Governance and/or the ICT provider may require from time to time against importing viruses or compromising system security.

Our 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 our data protection policy.

School social media accounts

The Trust has an official LinkedIn page, and each school has an official Twitter page, managed by the Trust Marketing & Communications Manager. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Monitoring of school network and use of ICT facilities

The Trust reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

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

The Trust monitors ICT use in order to:

- Obtain information related to school business.
- Investigate compliance with school policies, procedures and standards.
- Ensure effective school and ICT operation.
- 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.

Filtering and monitoring, compliant with the requirements of Keeping Children Safe in Education DfE Statutory guidance is in operation with the Trust. The reports generated as a result of filtering and monitoring activities are only accessible to authorized users.

6. Pupils

Access to ICT facilities

- Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music, or design and technology, must only be used 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 by using an assigned URL.

Search and deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

Unacceptable use of ICT and the internet outside of school

The school will sanction pupils and students, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on school premises):

- 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.
- Using ICT or the internet to breach Trust or school policy or procedures.
- Any illegal conduct, or 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 and 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 Trust or school, or risks bringing the Trust or 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) unauthorised access to the school's ICT facilities.
- Causing intentional damage to ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorization.
- Using inappropriate or offensive language.

This list is not exhaustive, and the Trust reserves the right to amend the list at any time.

7. Parents

Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents working for, or with the school in an official capacity (for instance, as a volunteer or as a member of a PTA (Parent & Teacher Association) or SPRB (School Performance Review Board)) may be granted an appropriate level of access, or be permitted to use the school's facilities at the headteacher's or Head of Governance's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

Communicating with or about the school online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

We ask parents to abide by the content of Appendix 2.

8. Data security

The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure, making use of multi-factor authentication settings wherever possible.

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

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

Passwords are allocated by the ICT provider. It is the responsibility of the individual assigned that password to protect it and change it in accordance with the password protocol outlined in the Information Policy.

Software updates, firewalls and anti-virus software

All Trust ICT devices that support software updates, security updates and anti-virus products 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 we implement and maintain to protect personal data and the Trust's ICT facilities.

Any personal devices using the Trust network must all be configured in this way.

Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's Information Policy.

Access to facilities and materials

All users of Trust ICT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by the Head of Governance.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Head of Governance immediately.

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 closed down completely at the end of each working day.

Particular care should be taken around using systems in the classroom environment or other public areas, with 'presenter mode' settings used for any system that contains personal or sensitive information to avoid a data breach occurring and to actively protect the confidentiality of information held by the Trust or school.

Encryption

The Trust ensures that all devices and systems have an appropriate level of encryption.

School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher or Head of Govrnance.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined by the ICT provider.

9. Protection from cyber attacks

Please see the glossary (appendix 3) to help you understand cyber security terminology.

The Trust and school will:

- Work with the Head of Governance and the ICT provider to make sure cyber security is given the time and resources it needs to make the school secure.

- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the school's annual training window) on the basics of cyber security.

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.

- Work with the Head of Governance and the ICT provider to investigate whether our IT software needs updating or replacing to be more secure.

- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data, they should report this immediately to the Head of Governance.

The Head of Governance and the ICT provider will:

- Put controls in place that are:

    - **'Proportionate'**: the Trust will verify this using a third-party audit, at least annually, to objectively test that what it has in place is up to scratch.
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe.
    - **Up-to-date**: with a system in place to monitor when the school needs to update its software.
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be.

- Back up critical data and store these backups on either cloud based backup systems and/or external hard drives that aren't connected to the school network and which can be stored off the school premises.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the ICT provider.

- Make sure staff:

    - Dial into our network using a virtual private network (VPN) when working from home, or via the Cloud.
    - Enable multi-factor authentication where they can, on things like school email.

- Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights.

- Have a firewall in place that is switched on.

- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification.

- Develop, review and test an incident response plan with the ICT provider for example, including how the school will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

10. Internet access

The Trust wireless internet connection is secured and should only be accessed using an allocated works device.

Parents and visitors

Parents and visitors to the Trust or school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the Headteacher or Head of Governance.

The Headteacher/Head of Governance will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA or SPRB)
- 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). A one-off access code will be provided to facilitate access.

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

11. Monitoring and review

The Head of Governance monitors the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the Trust. This policy will be reviewed annually.

12. Related policies

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

- Online safety
- Safeguarding and child protection
- Behaviour
- Discipline
- Information
- Cyber Security

Appendix 1: Facebook cheat sheet for staff

10 rules for school staff on Facebook

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 not, ensure that the image is professional.
3. Check your privacy settings regularly.
4. Be careful about tagging other staff members in images or posts.
5. Don't share anything publicly that you wouldn't be happy showing to pupils.
6. Don't use social media sites during working/school hours.
7. Don't make comments about your job, your colleagues, or school or your pupils online.
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, your personal email address or mobile number is able to find you using this information.
10. Consider uninstalling the Facebook app from your phone. The app recognises Wi-Fi connections and makes friend suggestions based on who else uses the same Wi-Fi connections, such as parents 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.
- 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.
- 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 the headteacher and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages.
- Notify the Headteacher about what is happening.

A parent 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 have indirect access through their parent’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, our disciplinary and behaviour policies are usually sufficient to deal with online incidents.
- If the perpetrator is a parent 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

Online channels are an important way for parents/carers to communicate with, or about, our school and Trust. The Trust/School uses the following channels:

- Our official Twitter pages.
- Our official LinkedIn page.
- DoJo/MCAS/Classcharts, Tapestry, text, email.

Parents/carers may also set up independent channels to help them stay on top of what's happening in their child's class/school. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, we expect that parents 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.

We expect that parents will not:

- Use private groups, the school's Twitter/LinkedIn pages, 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 if they are not raised in an appropriate way.
- Use private groups, the school's Twitter/LinkedIn pages, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. We expect you to contact the school and speak to the appropriate member of staff if you are aware of a specific behaviour issue or incident.
- Upload or share photos or videos on social media of any child other than my own, unless they have the permission of other children's parents/carers.

Appendix 3: Glossary of cyber security terminology

These key terms will help understand the common forms of cyber-attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration testing. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using two or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.

Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.