The Piggott School: Wargrave

‘Go and do Likewise’ Luke 10:25-37, The Parable of the Good Samaritan

We live with love and compassion, seeking help in times of need.

IT and Acceptable Usage Policy

Author:	DPO and Network Manager
Approver:	Local Governing Committee
Date:	11th November 2025
Next review:	November 2029 or earlier if there are technology advances or updated legislation or guidance
Category of policy:	Local Governing Committee

Changes history

Version:	**Date:**	**Amended by:**	**Substantive changes:**	**Purpose:**
2	Autumn 2025	Exams Officer and Governance Professional	Additional wording in the section on cyber security. Reference to Agape Trust policies	To incorporate the new JCQ regulations 2025-26 and new Agape Trust policies

Contents

1. Introduction and aims

Information and communications technology (IT) is an integral part of the way our school operates, and is a critical resource for pupils, staff (including the senior leadership team), governors, volunteers and visitors. It supports teaching and learning, and the pastoral and administrative functions of the school.

However, the IT resources and facilities our school uses could also pose risks to data protection, online safety, cyber security and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school IT resources for staff, pupils, parents/carers and governors
- Establish clear expectations for the way all members of the school community engage with each other online
- Support the school's policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of IT systems
- Support the school in teaching pupils safe and effective internet and IT use

This policy covers all users of our school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our:

- Behaviour (pupil) management policy
- Staff disciplinary policy and procedures
- Staff code of conduct
- Governor 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 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
- Keeping children safe in education 2025
- 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
- UK Council for Internet Safety (et al.) 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
- JCQ regulations 2025-26

3. Definitions

- **IT 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 that may become available in the future which is provided as part of the school's IT service
- **Users:** anyone authorised by the school to use the school's IT facilities, including governors, staff, pupils, volunteers, contractors and visitors
- **Personal use:** any use or activity not directly related to the users' employment, study or purpose agreed by an authorised user
- **Authorised personnel:** employees authorised by the school to perform systems administration and/or monitoring of the IT facilities
- **Materials:** files and data created using the school's IT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs

See appendix 4 for a glossary of cyber security terminology.

4. Unacceptable use

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

Unacceptable use of the school's IT facilities includes:

- Using the school's IT facilities to breach intellectual property rights or copyright
- Using the school's IT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's or Trust's policies or procedures

- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- 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 school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community
- Connecting any device to the school's IT network without 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 programme, tool or item of software designed to interfere with the functioning of the school's IT 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 IT facilities
- Causing intentional damage to the school's IT facilities
- Removing, deleting or disposing of the school's IT equipment, systems, programmes 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 school
- Using websites or mechanisms to bypass the school's filtering or monitoring mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, antisemitic or discriminatory in any other way
- Failing to adhere to the Trust's AI policy

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher will use their professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the school's IT facilities.

4.1 Sanctions

Pupils and staff who engage in any of the unacceptable activities listed above may face disciplinary action in line with the school's policies listed above.

Sanctions in place for unacceptable IT use include (but are not limited to) detention, suspension, revoking permission to use the school's systems, blocking access to the guest Wi-Fi and blocking access to certain websites.

The School's behaviour policy can be found on the school website. The staff code of conduct and staff disciplinary policy can be found on staff resources (sharepoint). The governor code of conduct is shared with governors annually and when it is updated. It can also be found on governor resources.

5. Staff (including governors, volunteers and contractors)

5.1 Access to school IT facilities and materials

The school's network manager manages access to the school's IT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's IT facilities.

Staff who have access to files that they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the network manager.

Staff who need additional access to IT systems should have their line manager or the owner of the system/shared folder request the IT Support Team to make appropriate changes.

5.1.1 Use of phones and email

The school provides each member of staff with an email address.

This email account should be used for work purposes only. Staff must enable multi-factor authentication on their email account(s).

All work-related business should be conducted using the email address the school has provided.

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

Staff 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.

Staff 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.

If staff 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 IT support team immediately and follow our data breach procedure which can be found in the data protection policy in staff resources or on the school website.

Staff must not give their personal phone number(s) to parents/carers 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 IT acceptable use as set out in section 4.

5.2 Personal use

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

Personal use is permitted provided that such use:

- Does not take place during contact 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 IT 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 IT facilities for personal use may put personal communications within the scope of the school’s IT 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 school’s Bring your Own Device policy.

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

Staff should take care to follow the school’s guidelines on use of social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

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

The school has recommendations for staff on appropriate security settings for all social media platforms (see appendix 1).

5.3 Remote access

Staff and Pupils (from Year 10 onward) can access the school's IT facilities and materials remotely.

We have two means of accessing our systems remotely, Staff VPN or Remote apps.

- Both systems are run by the IT support team – 221 or technical@piggottschool.org
- VPN access is only allowed from School owned Laptops, maintained by the IT support team.
- Both systems use the HTTPS protocol so are secured by 2048bit SSL encryption which will not get blocked by other schools or home Wi-Fi setups.
- Staff Laptops will come with the VPN software configured, remote apps can be setup by any end user, using the instruction sheets on the Pupils SharePoint (linked at the bottom of the school website)

People accessing the school's IT 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 IT facilities outside the school and must take precautions such as avoiding being overlooked by the public when sensitive information is on screen.

Our IT 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.

The School's data protection policy can be found on the Policies page of the school website.

5.4 School social media accounts

The school has an official Instagram account and a LinkedIn alumni account managed by Miss Lucy Reynolds (Assistant Headteacher). Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access, the account.

The school has guidelines for what may and must not be posted on its social media accounts. Those who are authorised to manage, or post to, the account must make sure they abide by these guidelines at all times.

5.5 Monitoring and filtering of the school network and use of IT facilities

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

- Internet sites visited
- Bandwidth usage
- Email accounts
- User activity/access logs

- Any other electronic communications

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

We use the software "Impero" to log internet activity of loaned and on-site IT equipment, as well as office 365 audit logging, firewall logs, authentication logs, IP logging, Print and File access logging to have a full picture as feasibly possible of activities on our systems.

The school monitors IT use to:

- Maintain safeguarding responsibilities
- Investigate compliance with school policies, procedures, and standards
- Ensure effective school and IT operation
- Conduct training or quality control exercises
- Prevent or detect cyber crime
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation
- Obtain information related to school business

Our Local Governing Committee is responsible for making sure that:

- The school meets the DfE's filtering and monitoring standards
- Appropriate filtering and monitoring systems are in place
- Staff are aware of those systems and trained in their related roles and responsibilities
    - For the leadership team and relevant staff, this will include how to manage the processes and systems effectively and how to escalate concerns
- It regularly reviews the effectiveness of the school's monitoring and filtering systems

The school's designated safeguarding leads (DSL's) will take lead responsibility for understanding the filtering and monitoring systems and processes in place.

Where appropriate, staff may raise concerns about monitored activity with the school's DSL and IT manager, as appropriate.

6. Pupils

6.1 Access to IT facilities

- Computers and equipment in the school's IT Classrooms are available to pupils only under the supervision of staff
- Open areas for drop in access are available in the Library and 6th Form Common Room

- Specialist IT equipment, such as that used for Music, Photography or Design and Technology must only be used with the agreement of staff within the department that it is located within.
- Pupils will be provided with an account linked to all the school's cloud systems, which they can access from any device by using the following URLs

  https://portal.office.com
  https://www.piggottapps.co.uk/rdweb
  https://classroom.google.com

6.2 Search and deletion

Under the Education Act 2011, the Headteacher, and any member of staff authorised to do so by the Headteacher, can search pupils and confiscate their mobile phones, computers or other devices that the authorised staff member has reasonable grounds for suspecting:

- Poses a risk to staff or pupils, **and/or**
- Is identified in the school rules as a banned item for which a search can be carried out (our behaviour policy lists these items), and/or
- Is evidence in relation to an offence

This includes, but is not limited to:

- Pornography
- Abusive messages, images or videos
- Indecent images of children
- Evidence of suspected criminal behaviour (such as threats of violence or assault)

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Assess how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the Headteacher / Designated Safeguarding Lead.
- Explain to the pupil why they are being searched, and how and where the search will happen, and give them the opportunity to ask questions about it
- Seek the pupil's co-operation (if the pupil refuses to co-operate, we will proceed according to our behaviour policy

The authorised staff member will:

- Inform the DSL (or deputy) of any searching incidents where they had reasonable grounds to suspect a pupil was in possession of a banned item.
- Involve the DSL (or deputy) without delay if they believe that a search has revealed a safeguarding risk

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on a device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on a device, the staff member should only do so if they reasonably suspect that the data has been, or could be, used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / Headteacher / other member of the SLT to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding whether there is a good reason to erase data or files from a device, staff members will consider whether the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as is reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, **and/or**
- The pupil and/or the parent refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- **Not** copy, print, share, store or save the image
- Confiscate the device and report the incident to the DSL (or deputy) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on searching, screening and confiscation and the UK Council for Internet Safety (UKCIS) et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of pupils will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS et al.'s guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Our Behaviour Policy

Any complaints about searching for, or deleting, inappropriate images or files on pupils' devices will be dealt with through the school complaints procedure.

6.3 Unacceptable use of IT and the internet outside of school

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

- Using IT or the internet to breach intellectual property rights or copyright
- Using IT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's or Trust'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) unauthorised access to the school's IT facilities
- Causing intentional damage to the school's IT 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

7. Parents/carers

7.1 Access to IT facilities and materials

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

However, parents/carers working for, or with, the school in an official capacity (for instance, as a volunteer or as a member of the PSA) 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.

7.2 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/carers 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.

7.3 Communicating with parents/carers about pupil activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out.

When we ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

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.

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

8. Data security

The school 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.

Staff, pupils, parents/carers and others who use the school's IT facilities should always use safe computing practices. We aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges, including the use of:

- Firewalls
- Security features
- User authentication and multi-factor authentication
- Anti-malware software

8.1 Passwords

All users of the school's IT facilities should set strong passwords for their accounts and keep these passwords secure. Staff passwords must be set to that they contain both uppercase and lowercase letters, as well as a number and/or a symbol. Pupils should be encouraged to do the same but are not enforced beyond needing more than 5 characters in their password.

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, visitors or volunteers who disclose account or password information may have their access rights revoked.

Staff and pupils are allocated a password when they first start with the school, which is required to be changed annually.

8.2 Software updates, Firewalls and Anti-Virus software

All the school's IT devices that support software updates, security updates and anti-virus products will have these installed and 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 school's IT facilities.

Any personal devices using the school's network must all be configured to get updates and install them regularly.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the school's data protection policy.

The Schools Data Protection Policy can be found on the Policies page of the School Website.

8.4 Access to facilities and materials

All users of the school's IT facilities will have clearly defined access rights to school systems, files and devices.

These access rights are managed by The IT Manager.

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 IT Support Team 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 shut down completely at the end of each working day.

8.5 Encryption

The school makes sure that its 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.

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

9. Protection from cyber attacks

Please see the glossary (appendix 6) to help you understand cyber security terminology.

The Piggott School is a large-sized secondary school with an on-site IT support team. Staff regularly use awarding organisation systems: JCQ, AQA, Pearson Edexcel and OCR, NCFE Eduqas portals, as well as the school's Management Information System (MIS) and Microsoft 365 for email and document sharing. Cyber security responsibilities are coordinated by the IT Manager, with the Head of Centre and Exams Officer holding specific responsibility for secure access to awarding organisation platforms. All measures within this policy are tailored to reflect the school's size, staffing structure, and use of cloud-based technologies, and are informed by guidance from the National Cyber Security Centre (NCSC) for education settings.

The school will:

- Work with governors and the IT department 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, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information

  This annual training will specifically include requirements for all staff who access awarding organisation systems to ensure they understand and comply with the security expectations of those platforms. We will also make sure that certificates of completed cyber security training are collated and are kept for inspection by JCQ.

- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- 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
- Put controls in place that are:
    - **Proportionate:** the school will verify this using a third-party audit (such as 360 degree safe) annually, to objectively test that what it has in place is effective
    - **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 effective and secure as they can be
- Back up local and critical data nightly, store backups on a separate server and later copy to tape. All data from school databases and shared drives should be made available for recovery for several months.
- Cloud backups of OneDrive and email operate on a 2-year retention – i.e. only Exchange and OneDrive data created or modified in the past 2 years is available on the Cloud backup system. Whole school SharePoint sites will have their content backed up with a 5-year retention period. This is to ensure cost effectiveness of the backup solution whilst still retaining critical functionality.

- Delegate specific responsibility for maintaining the security of our management information system (MIS) to the IT Manager
- Make sure staff are encouraged to:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like school email accounts and the payroll account login
    - Store passwords securely using a password manager such as those built into Google Chrome or Microsoft Edge browsers.
- Make sure IT 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 configured appropriately.
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and checking if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT Department including, for example, how the school will communicate with everyone if communications go down, who will be contacted and when, and who will notify Action Fraud of the incident. This plan will be reviewed and tested annually and after a significant event has occurred, using the NCSC's 'Exercise in a Box'
- Work with our Local Authority – Wokingham District Council - to see what it can offer the school regarding cyber security, such as advice on which service providers to use or assistance with procurement

10. Internet access

The school's wireless internet connection is secure.

- Filtering is in place on the guest network – the level of access is determined by your login and will be the same filter level as when you are using a school computer.
- Devices on the guest network are prevented from talking to each other to prevent the transmission of viruses
- Guests will need a logon providing for them to access the Wi-Fi which should be arranged with IT support by the member of staff that they are visiting before their date of arrival.
- If you find you are being filtered when you think you should not be, please contact technical@piggottschool.org who will review and update the filter as appropriate.

10.1 Pupils

Pupils in all year groups are allowed to access the Bring Your Own Device network.

- Wi-Fi is available across the site
- Use of the Wi-Fi is limited to educational activities only.

- Access can be withdrawn at any time should a complaint be made to the IT Support Team or if the IT Support Team are alerted by the system logs of suspicious activities or malware.
- Devices connected to the Bring your own device Wi-Fi need to have MAC randomisation turned off – on Apple devices this setting is called “Private IP” and “Limit IP tracking”, which must both be turned off to maintain a connection.   This is because our system needs to identify you to give you appropriate levels of access to the internet.

10.2 Parents/carers and visitors

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 or if there is a public event that Wi-Fi has been arranged for.

The Headteacher will only grant authorisation if:

- Parents/carers are working with the school in an official capacity (e.g. as a volunteer or as a member of the PSA)
- Visitors need to access the school’s Wi-Fi 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 School Equipment or PGCE Wi-Fi Network password to anyone, doing so could result in disciplinary action.

11. Monitoring and review

The Headteacher, DPO and IT Manager monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 4 years or earlier if required.

The Local Governing Committee is responsible for reviewing and approving this policy.

12. Related policies

This policy should be read alongside the school’s and Trust’s policies on:

- Behaviour (pupil) management policy
- Staff disciplinary policy and procedures
- Staff code of conduct
- Data Protection Policy
- AI
- Governor code of conduct
- Child protection and safeguarding
- Bring your own device

Appendix 1: Facebook advice sheet for staff

Do not accept friend requests from pupils on social media

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 you don't, make sure 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 your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our 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) can 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 connection (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** – please go to bit.ly/2MdQXMN so you can 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 1 parent/carer'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/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/carer 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 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 agreement for pupils

**Acceptable use of the school's IT facilities and internet:
agreement for pupils**

Name of pupil:

When using the school's IT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites,
- Attempt any Hacking or Doxing
- Access social networking sites
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share any inappropriate images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people

Our school abides by the JCQ AI Use in Assessments Policy, therefore I will not:

- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
  - During assessments, including internal and external assessments, and coursework
  - To present AI-generated text or imagery as my own work

I understand that the school will monitor the websites I visit and my use of the school's IT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the school's IT systems and internet responsibly.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):	**Date:**

Parent/carer agreement: I agree that my child can use the school's IT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's IT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.	
Signed (parent/carer):	**Date:**

Appendix 3: Glossary of cyber security terminology

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

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
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.
Doxing	A practice where individuals or groups expose and publicise private information about a person on the internet without their consent, often for the purposes of causing distress or creating malicious intent.
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.

TERM	DEFINITION
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 test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as 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 a 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 2 or more different components to verify a user's identity.

TERM	DEFINITION
Virus	Programmes 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 people in an organisation.