PINNER
HIGH SCHOOL

Policy	ICT, Internet Acceptable Use and AI Policy
Date of Review	May 2025
Reviewed By	Head of ICT
Date of Approval	*Pending*
Approved By	LGB
Date of Next Review	May 2027
Statutory/Non Statutory	Non Stat
Website/Non Website	Website

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

However, the ICT resources and facilities our school uses also pose risks to data protection, online safety and safeguarding.

This policy aims to:

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

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

Breaches of this policy may be dealt with under our behaviour policy.

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 2018
- Searching, screening and confiscation: advice for schools

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 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 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 output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered *unacceptable* use of the school'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 school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies 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
- 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 ICT 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 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 school
- Using websites or mechanisms to bypass the school's filtering mechanisms

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

4.1 Exceptions from unacceptable use

Where the use of school ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

Anybody who seeks to apply for an exemption should set out their request in writing and email it to the headteacher with a minimum of 3 days notice.

4.2 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 on student behaviour and staff conduct.

5. Staff (including governors, volunteers, and contractors)

5.1 Access to school ICT facilities and materials

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

- Computers, tablets and other devices
- Access permissions for certain programmes 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 Senior ICT Technician.

Staff will need to make such requests by raising a ticket using Parago.

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.

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 and 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 which contains the personal information of another person, they must inform the Head of Operations, the Data Manager and the Network Manager immediately and follow our data breach procedure.

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.

5.2 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. A member of SLT or IT Team 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 teaching hours

- 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 monitoring activities (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.

Staff should not use personal devices (such as mobile phones, home computers or tablets) to access school email, communications, documents or systems where this can be avoided. If they do so :

- they should take all reasonable care to protect the privacy and confidentiality associated with school communications, documents and systems
- they must only access the school network from a device with personal password protection
- they should not access the school network from a home (or other shared) computer with shared log on or access
- they should not leave the device unlocked/open where this would allow non employees to access to school email, communications, documents or systems
- they should avoid downloading documents onto personal devices and if they do so, they should delete the download from the personal device as soon as possible

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 school’s guidelines on 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 ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Staff should ensure they do not accept any friend/follow requests from students or parents and should ensure their public/private security settings are appropriate. The school has guidelines for staff on appropriate security settings for social media accounts (see Appendix 1).

5.3 Remote access

We allow staff to access the school’s ICT facilities and materials remotely.

This facility is only available to members of staff that have been allocated a school Laptop as part of their duties and protected with Encryption.

We use a VPN which requires the IT Department to install a certificate and configure the connection on the staff laptop. This then needs to be connected to, along with an internet connection, before access to the network is granted remotely.

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 the IT Support Team 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.

https://www.pinnerhighschool.org/attachments/download.asp?file=1650&type=pdf

Staff should not use personal devices (such as mobile phones, home computers or tablets) to access school email, communications, documents or systems where this can be avoided. If they do so

- they should take all reasonable care to protect the privacy and confidentiality associated with school communications, documents and systems they must only access the school network from a device with personal password protection
- they should not access the school network from a home (or other shared) computer with shared log on or access
- they should not leave the device unlocked/open where this would allow non employees to access to school email, communications, documents or systems
- they should avoid downloading documents onto personal devices and if they do so, they should delete the download from the personal device as soon as possible

5.4 School social media accounts

The school has an official Facebook, Instagram and Twitter page, managed by the Head of IT. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account. Those who are authorised to manage the account must ensure that they do so in accordance with the principles of acceptable/unacceptable use set out in this policy.

5.5 Monitoring of school network and use of ICT facilities

The school 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/Print/Data usage
- Email accounts
- Telephone calls
- 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 school 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

5.6 Use of USB memory drives/storage devices

Any USB memory drive/storage device should only be used for backup purposes, and need to be scanned by the IT Department before use. All files need to be uploaded to Google Drive instead of using USB Memory drives/storage devices.

6. Pupils

6.1 Access to ICT facilities

- Computers and equipment in the school's ICT suite, Year group communal areas and LRC are available to pupils only under the supervision of staff
- Specialist ICT equipment, such as that used for music or design and technology including Laser Cutter/3D Printers must only be used under the supervision of staff
- Pupils will be provided with a login account linked to the school's network and virtual learning environment Google Suite, which they can access from any device by using the following URL https://gsuite.google.co.uk/
- Students who have signed an AUP (Acceptable Use Policy) have been provided with a school email address which they must use responsibly and appropriately for school-related matters only
    - This email account should be used for school-related purposes only.
    - All school-related business should be conducted using the email address the school has provided.
    - Students must not share their personal email addresses with staff and must not send any work-related materials using their personal email account.
    - Students 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 sometimes 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.
    - Students 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 a student receives 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 a student sends an email in error which they think they should not have sent, they must inform their form tutor immediately.

6.2 Search and deletion

Under the 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.

6.3 Unacceptable use of ICT and the internet outside of school

The school will sanction pupils, 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
- Breaching the school's policies 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
- 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 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 authorisation
- Using inappropriate or offensive language
- Use of USB memory drives/storage devices is prohibited

Sanctions will be applied following the school's behaviour policy.

6.4 Bring Your Own Device (BYOD) – Sixth Form Students

As part of our commitment to supporting independent learning at PHS, Sixth Form students are required to bring their own devices (Laptops or Chromebooks) for use in school. However, the following conditions apply:

Device Security & Usage

- All devices must be connected to the PHS designated 6th Form SSID.
- Personal devices must only be used for educational purposes and in line with the school's IT policies.
- Students are responsible for ensuring their devices do not contain inappropriate or illegal content.

Network Access & Monitoring

- The school reserves the right to monitor network activity to ensure compliance with our IT policies.
- Students must not attempt to bypass security settings, firewalls, or filtering systems.
- The school's IT support team will not be responsible for troubleshooting personal device issues.

Liability & Responsibility for Damage or Loss

- Students are fully responsible for the security and maintenance of their own devices.
- The school accepts no liability for loss, theft, or damage to personal devices brought onto school premises.
- Devices and chargers should be kept secure at all times.
- In cases of accidental damage caused by another student, this must be reported immediately, but the school will not be held responsible for costs related to repairs or replacements.

By bringing a personal device into school, students agree to adhere to this policy and understand that failure to comply may result in the loss of BYOD privileges.

6.5 Student Loaned Devices

The school is committed to ensuring all students have equal access to digital learning. To support this, we provide loaned Chromebooks to students who do not have access to a suitable device at home. The following conditions apply:

Eligibility & Loan Agreement

- Devices are allocated on a case-by-case basis and subject to availability.
- A loan agreement must be signed by the students parent/carer before a device is issued.
- Devices remain the property of the school and must be returned (in its original condition) upon request.

Acceptable Use & Responsibilities

- The device must remain at home and not brought into school
- The device must only be used for educational purposes and in line with the school's IT Acceptable Use Policy.
- Students are responsible for ensuring the device is used safely and appropriately.
- The device must not be altered, tampered with, or have unauthorised software/extensions installed.

Care & Security

- Students must take reasonable care to prevent damage, loss, or theft.
- Devices should be stored securely when not in use and never left unattended in public places.
- If a device is lost, stolen, or damaged, it must be reported to the school immediately.

Liability & Costs

- The school will carry out routine maintenance and repairs for faults that occur through normal use.
- In cases of damage caused by negligence, misuse, or loss, the student's parent/carer may be liable for repair or replacement costs.
- Failure to return a device when requested may result in the school seeking reimbursement.

By accepting a loaned device, students and parents/carers agree to these terms. Failure to comply may result in the withdrawal of the device loan and further action as necessary.

7. Parents

7.1 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 an employee volunteer or as a member of the PTA) may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion. Where this is permitted, there must always be appropriate regard to data protection, privacy and confidentiality. Where parents 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 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 sign the agreement in Appendix 2.

8. Data security

The school takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee the security of these items. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure. These passwords are set to expire every 90 days.

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.

8.2 Software updates, firewalls, and anti-virus software

All of the school's 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 school's ICT facilities.

Any personal devices using the school's network must all be configured in this way.

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 which can be found on the School's website.

8.4 Access to facilities and materials

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

These access rights are managed by the Network Manager and the IT team, in consultation with the Head of IT.

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 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 closed down completely at the end of each working day.

Users should not save their passwords when prompted by Google, for example, on public computers as it opens the risk of other users accessing unauthorised accounts.

8.5 Encryption

The school ensures that its devices and systems have an appropriate level of encryption using Bitlocker.

School staff may only use personal devices (including computers or tablets) 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 Network Manager.

9. Internet access

The school wireless and Wired internet connection is secured.

We use an MDM solution for our iPads and an internal and external firewall to protect the School Network.

Pinner High also has its internet gateway managed and filtered by London Grid for Learning “LGFL”.

Everyone has access to the same internet connection, students and staff alike, but only while using school ICT Equipment. On occasion we do have a separate Guest Wi-Fi for consultants and visitors to the school who need to access their content, this service has limited support only and we advise guests and visitors to check content/websites before they arrive on site with the contact they are meeting or providing work for.

If a site is not blocked or needs to be blocked as it is inappropriate this needs to be communicated with the IT Team via a Parago Helpdesk ticket. All members of staff have access to log Helpdesk tickets via the Parago system.

9.1 Pupils

Pupils are NOT permitted to use school wifi on their personal devices with the exception of Sixth form students who will be required to see the IT Department who will connect their device to a designated SSID.

9.2 Visitors

Visitors to the school will only be permitted to use the school’s wifi in exceptional circumstances and with the headteacher’s authorisation.

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

10. Artificial Intelligence (AI)

The use of generative AI within education is evolving, and we recognise that it presents both opportunities and challenges for staff and students.

10.1 Generative AI for Staff

We encourage staff to explore generative AI tools and consider how they can enhance teaching and learning. Staff are also encouraged to make use of generative AI to reduce workload, both in delivering the curriculum and in non-student-facing tasks.

Staff should remain mindful of the limitations of generative AI tools and must apply professional judgement when using them. Any content generated using AI must be reviewed for accuracy, appropriateness, and relevance. Regardless of the tools used, the quality and appropriateness of all materials produced remain the professional responsibility of the individual who created them.

Access to generative AI platforms is not restricted on staff devices. The use of AI is acceptable within the following parameters:

Staff must:

- only create accounts on AI platforms for work-related purposes using their school email address or school-linked Google account;
- acknowledge any use of AI in the creation of teaching materials or resources;
- not input any personal data, including student details, staff details, or their own personal information, into AI platforms;
- not enter student work into AI platforms where user inputs may be used to train large language models (LLMs);
- not use AI to mark or grade student work without student consent (although it may be used to support aspects of assessment, such as feedback drafting or rubric design);

10.2 Safeguarding, Data Protection, and Responsible Use

The use of AI must always align with our safeguarding and data protection policies. Staff must not input any personally identifiable information (PII) about students, colleagues, or themselves into AI tools, especially those hosted outside the UK or using data for training purposes. This includes names, email addresses, dates of birth, student work, SEN information, or any other data considered sensitive under UK GDPR.

Staff are advised to check the terms of service and privacy policies of AI platforms before using them. If in doubt, guidance should be sought from the Data Protection Officer (DPO) or a member of the senior leadership team.

Examples of responsible AI use include:

- Generating differentiated comprehension questions from a shared source text;
- Drafting exemplar answers for class discussion or modelled writing;
- Creating lesson starter prompts or recap quizzes;
- Generating feedback templates or suggested feedback phrasing (to be edited by the teacher);
- Supporting curriculum planning by offering ideas for sequencing or resource suggestions.

AI should be viewed as a supportive tool rather than a replacement for professional expertise. Human oversight and pedagogical judgement must always remain central.

10.3 Use of AI with Students

When students are using devices, staff must monitor activity using Impero or the relevant network monitoring software. Particular vigilance is required when students are using generative AI platforms.

Students may access a range of AI tools, including (but not limited to) ChatGPT, Microsoft Copilot, Google Gemini, and tools integrated into platforms such as Canva or Microsoft Word. This list is not exhaustive, and the availability of AI tools is rapidly evolving. Staff should be mindful of the age restrictions associated with these platforms. For example, OpenAI's ChatGPT requires users to be 13 or older, and Microsoft Copilot requires users to be 18 or older. Staff must not encourage or facilitate student use of platforms where age restrictions are not met. Any recommendation of AI tools for student use must be appropriate and compliant with relevant terms of service.

Staff are encouraged to engage in open discussion with students about the appropriate, ethical, and transparent use of generative AI. These discussions should include both the opportunities AI presents for learning and productivity, as well as its limitations, potential for misinformation, and risks to academic integrity.

All work submitted by students for assessment must be their own. If students use generative AI to support their work for example, to generate ideas, draft text, or check grammar - this must be clearly acknowledged. Failure to acknowledge the use of AI constitutes malpractice.

If a member of staff suspects that a piece of work includes AI generated content, the matter should first be discussed with the student. The student should be given an opportunity to amend and resubmit the work with appropriate acknowledgement. If the resubmitted work still includes unacknowledged AI content, usual departmental procedures for non-completion of homework or misconduct should be followed.

10.4 AI Use in NEA and External Assessment

In line with JCQ guidance, students must not use generative AI in any way that constitutes malpractice in Non-Exam Assessment (NEA) or public examinations. This includes, but is not limited to, using AI to generate written responses, code, data analysis, design work, or other assessed content.

Students are permitted to use AI to support general research, ideation, or proofreading only if this is explicitly permitted by the exam board's subject-specific guidance and such use must be fully acknowledged in the candidate's work.

Any unauthorised or unacknowledged use of generative AI in NEA or exams will be treated as a serious breach of examination regulations and reported in line with our Exams Policy and the JCQ Malpractice Framework.

Staff must familiarise themselves with the school's Exams Policy and the most up-to-date JCQ guidance when supervising NEA or supporting exam-related work.

11. Monitoring and review

The headteacher and Head of IT with the help of the Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

12. Related policies

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

- E-Safety Policy
- Safeguarding and child protection Policy

- Behaviour Policy
- HR Policy
- Data Protection Policy
- CCTV
- Non-examination Assessment (including controlled assessment and coursework) Policy
- Other relevant policies in place from time to time

Head of ICT

May 2025

Appendix 1: Social Media Guidance for Staff

1. Change your social media 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 - always ensure your privacy settings are appropriate and strictly limited
4. Be careful about tagging other staff members in images or posts
5. Always ensure any content you create or share is appropriate : don't share anything publicly that you wouldn't be happy showing your employer, colleagues, pupils or parents
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
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 - these apps recognise Wi-Fi connections and makes friend/follow 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
- 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, screenshot, 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
- Email the DSL to notify them of what has happened and complete a safeguarding form and hand it to DSL at your earliest opportunity.

- If the pupil asks you about the friend/follow 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. If the pupil persists, take a screenshot of their request and any accompanying messages

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 then 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 the relevant social network and ask them to remove it
- Report the issue to the headteacher or other member of SLT
- 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 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 should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Student Name: _____ Form _____

Pinner High School Student Acceptable Use Policy for ICT

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

Students of Pinner High promote the 'Pinner High Values' by being responsible users and staying safe while using the internet and other digital technologies for educational, personal and recreational use.

The Values are grouped into three sections:

- Myself: Kindness, compassion, integrity, balance, respect, trust
- My school: Creativity, enthusiasm, resilience, flexibility, dedication, perseverance
- My community: Responsibility, collaboration, open-mindedness, confidence, adaptability, courage

Bringing life to these Values means that good ICT practice is the responsibility of all in the school community – parents, staff, governors and students. The aim is that school systems and users are protected from accidental or deliberate misuse, or actions that could compromise the security of the systems and that students will have good access to digital technologies to enhance their learning.

1. General

- I understand that the School regularly monitors use of the ICT systems, email and other digital communications of all its users for my protection.
- I will only use the School's computers for schoolwork, homework and as directed.
- I will act as I expect others to act towards me. In particular, I will respect others' work and property, and will not access, copy, remove or otherwise alter any other user's files without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others. I will not use strong, aggressive or inappropriate language, and I appreciate that others may have different opinions.
- I will act responsibly in my use of social networking websites, and make sure that my posts do not bring the School into disrepute.
- I agree that my image or likeness can be used on the School website or in any promotional material published by the School or associated agencies, with permission of my parents via the photo permission form.
- Files are not to be brought in on removable media (such as flash drives etc.). You must use your online workspace or school email (if applicable) to send work to and from school.
- I will not eat or drink near computer equipment.

2. Cyberbullying

- Cyberbullying is the use of information and communication technologies, particularly mobile phones and the internet, to support deliberate, inappropriate behaviour by an individual or a group, which is intended to harm another individual or group. This may be on a single occasion or repeated over a period of time.

- I understand that the School considers cyberbullying a serious offence, both within and outside School. I will report any incident of cyberbullying to the Designated Person for Child Protection, which will be logged and followed up in accordance with the School's Anti-Bullying Policy.

3. Internet

- I will use the internet responsibly and will not visit websites I know to be banned by the School. I am also aware that during lessons I should only visit websites that are appropriate for my studies. If I am unsure if a site is safe I will ask a member of staff. The internet is NOT a secure means of transferring information.
- I will report any misuse of the internet immediately to a member of staff.
- I will not attempt to set-up or use any proxy by-pass software in order to by-pass the School internet filter. Any misuse could result in disciplinary action.
- I will not take information from the internet and pass it off as my own work (plagiarism and copyright infringement).
- I will be responsible for my use of email and any other electronic communications. I will not include any material that is inappropriate or use offensive or threatening language in my emails or in any other communication on the internet. I understand that any email going out from the School will carry the School address and so represents the School. School email addresses will remain active for only one year after graduation.
- I will be provided with a school email address which ~~they~~ I must use responsibly and appropriately for school-related matters only
    - This email account must be used for school-related purposes only.
    - All school-related business should be conducted using the email address the school has provided me.
    - I must not share my personal email addresses with staff and must not send any work-related materials using my personal email account.
    - I 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 sometimes 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.
    - I 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 I receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, I must not make use of that information or disclose that information.
    - If I send an email in error which I think they should not have sent, I must inform my form tutor immediately.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.
- I will not use the School ICT system for on-line gaming, on-line gambling, file sharing or video broadcasting.

4. Online Safety

- I will not give my home address, phone number, send photographs or video, or give any other personal information that could be used to identify me, my family or my friends, unless a trusted adult has given permission.

- I will never arrange to meet someone I have only ever previously met on the internet or by email or in a chat room, unless I take a trusted adult with me.
- If I see anything I am unhappy with or I receive a message I do not like (both in and out of School), I will not respond to it but I will save it and talk to a teacher/trusted adult.
- I am aware that some websites and social networks have age restrictions and I should respect this.
- I am aware that my online activity at all times should not upset or hurt other people and that I should not put myself at risk either when accessing the internet through the School network or through personal hardware (e.g. laptops and mobile phones).
- I will not attempt to impersonate another person online e.g. post comments and access online accounts (Facebook, webmail) belonging to someone else.

5. Network

- I will keep my logins, IDs and passwords secret. I will not share them, nor will I try to use any other person's username and password. If I feel that password security has been compromised, I will report this to the IT Department and change my password immediately.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes. Any suspicious emails should be reported to ICT support immediately.
- I will not bring files into School (on removable media or online) without permission or upload inappropriate material to Google Drive, Google Classroom or any other online workspace. I will immediately report any damage or faults involving equipment or software.
- I will not attempt to gain unauthorised access to any part of the School's network that is not available from my personal logon, either via the network or the internet. I will not attempt to use or load programmes, files, tools or shortcuts to gain access to restricted parts of the network. I will immediately report any instance where I have inadvertently gained access to restricted areas to a member of staff.

Parent/Carer

As the parent or legal carer of the above student, I have read the Acceptable Use Policy and grant permission for my son or daughter, or the child in my care, to access the School's ICT network and resources for educational purposes. I understand that while every reasonable precaution will be taken by the School to provide for online safety, the School cannot be held responsible if students access unsuitable websites.

Name ……

Signature ……

Date ……..

Student Name ……

Student Signature ……

Date ……..

Appendix 3 - E-Safety and ICT Acceptable Use Policy

E-Safety and ICT Acceptable Use Policy

Statement of intent
This policy has been developed to ensure that all adults at Pinner High School are working together to safeguard and promote the welfare of young people.

E-Safety is a safeguarding issue not an ICT issue and all members of the school community have a duty to be aware of e-safety at all times, to know the required procedures and to act on them.

This document aims to put into place effective management systems and arrangements which will maximise the educational and social benefit that can be obtained by exploiting the benefits and opportunities of using ICT, whilst minimising any associated risks. It describes actions that should be put in place to redress any concerns about student welfare and safety as well as how to protect young people and staff from risks and infringements.

The Headteacher or, in their absence, the authorised member of staff for e-safety has the ultimate responsibility for safeguarding and promoting the welfare of students in their care.

The purpose of internet use in school is to help raise educational standards, promote student achievement, and support the professional work of staff as well as enhance the school's management information and business administration systems.

The internet is an essential element in 21st century life for education, business and social interaction and the school has a duty to provide young people with quality access as part of their learning experience and curriculum.

A risk assessment will be carried out before young people are allowed to use new technology in the school.

Ethos
- It is the duty of the school to ensure that every student in its care is safe. The same 'staying safe' outcomes and principles outlined in the Every Child Matters agenda apply equally to the 'virtual' or digital world;
- Safeguarding and promoting the welfare of students is embedded in the culture of the school and its everyday practice and procedures;
- All staff have a responsibility to support e-Safe practices in school and all students need to understand their responsibilities in the event of deliberate attempts to breach e-safety protocols;
- E-safety is a concern that is not limited to school premises, school equipment or the school day;
- Bullying, harassment or abuse of any kind via digital technologies or mobile phones will not be tolerated and complaints of cyber-bullying will be dealt with in accordance with the school's policies on behaviour and preventing and responding to bullying;
- Complaints related to child protection will be dealt with in accordance with the school's child protection policy.

The Headteacher of Pinner High School will ensure that:
- All staff are included in E-Safety training. Staff must also understand that misuse of the internet may lead to disciplinary action (as detailed in section 5 of the HR Policies) and possible dismissal;
- A Designated Senior Member of Staff for E-learning /Safety is identified and receives appropriate on-going training, support and supervision and works closely with the Designated Person for Child Protection;
- All temporary staff and volunteers are made aware of the school's E-learning /Safety Policy and arrangements;

- A commitment to E-Safety is an integral part of the safer recruitment and selection process of staff and volunteers.

The Governing Body will ensure that:
- There is a senior member of the school's leadership team who is designated to take the lead on e-learning/safety within the school;
- Procedures are in place for dealing with breaches of e-safety and security;
- All staff and volunteers have access to appropriate ICT training.

Teaching and learning
Benefits of internet use for education:
- The internet is a part of the statutory curriculum and a necessary tool for staff and students and it benefits education by allowing access to worldwide educational resources including art galleries and museums, as well as enabling access to specialists in many fields for students and staff;
- Access to the internet supports educational and cultural exchanges between students worldwide and enables students to participate in cultural, vocational, social and leisure use in libraries, clubs and at home;
- The internet supports professional development for staff through access to national developments, educational materials, good curriculum practice and exchange of curriculum and administration data;
- The internet improves access to technical support, including remote management of networks, supports communication with support services, professional associations and colleagues as well as allowing access to, and inclusion in, government initiatives;
- The internet offers opportunities for mentoring students and providing peer support for them and their teachers;
- Students will be educated in the effective use of the internet in research, including the skills of knowledge location, retrieval and evaluation;
- Students will be encouraged to question what they read and to seek confirmation of matters of fact from more than one source. They will be taught research techniques including the use of subject catalogues and search engines and encouraged to question the validity, currency and origins of information. Students will also be taught that copying material is worth little without an appropriate commentary demonstrating the selectivity used and evaluating the material's significance;
- Students will be taught to acknowledge the source of information used and to respect copyright when using internet material in their own work.

Managing the internet
- Developing good practice in internet use as a tool for teaching and learning is essential. The School internet access will be designed expressly for student use and will include filtering appropriate to the age of the young people;
- Students will be taught what internet use is acceptable and what is not and be given clear objectives for internet use. Staff will guide students in on-line activities in class that will support the learning outcomes planned for the student's age and maturity;
- Students will be taught what to do if they experience material that they find distasteful, uncomfortable or threatening;
- If staff or students discover unsuitable sites, the URL (address) and content must be reported to the ICT Technician and Senior member of staff;
- The School will ensure that the use of Internet derived materials by staff and students complies with copyright law;
- Students will be taught to be critically aware of the materials they read as well as how to validate information before accepting its validity.

Managing email
- Personal email or messaging between staff and students should not take place;
- Staff must use the Google Classroom assignment comments if they need to communicate with students about their School work.

- Students and staff may only use approved email accounts on the school system and students must inform a member of staff immediately if they receive an offensive email;
- Students must not reveal details of themselves or others in any e-mail communication or by any personal web space such as an address, telephone number and must not arrange meetings with anyone;
- Access in School to external personal email accounts may be blocked;
- Excessive social email use can interfere with learning and will be restricted;
- The forwarding of chain letters is not permitted;
- Incoming email should be monitored and attachments should not be opened unless the author is known.

Managing website content

- Editorial guidance will ensure that the school's ethos is reflected in the website, information is accurate, well presented and personal security is not compromised. Care will be taken to ensure that all information is considered from a security viewpoint including the use of photographic material;
- Photographs of students will not be used without the written consent of the student's parents/carers;
- The point of contact on the school website will be the school address, School email and telephone number. Staff or students' home information will not be published;
- The Headteacher or nominated person will have overall editorial responsibility and ensure that all content is accurate and appropriate;
- The website will comply with the school's guidelines for publications and parents/carers will be informed of the school policy on image taking and publishing;
- Use of site photographs will be carefully selected so that any students cannot be identified or their image misused;
- The names of students will not be used on the website, particularly in association with any photographs;
- Work will only be used on the website with the permission of the student and their parents/carers;
- The copyright of all material must be held by the school or be attributed to the owner where permission to reproduce has been obtained;
- Students will be taught to consider the thoughts and feelings of others when publishing material to websites and elsewhere. Material which victimises or bullies someone, or is otherwise offensive, is unacceptable and appropriate sanctions will be implemented.

Social networking and chat rooms

- The School will control access to moderated social networking sites and educate students in their safe use;
- Students will not access social networking sites eg 'Twitter', 'Facebook' or 'Bebo' on site;
- Students will be taught the importance of personal safety when using social networking sites and chat rooms;
- Students will not be allowed to access public or unregulated chat rooms;
- Students will only be allowed to use regulated educational chat environments and use will be supervised;
- Newsgroups will be blocked unless an educational need can be demonstrated;
- Students will be advised to use nicknames and avatars when using social networking sites off site;
- Staff will not exchange social networking addresses or use social networking sites to communicate with students;
- Should special circumstances arise where it is felt that communication of a personal nature between a member of staff and a student is necessary, the agreement of a senior manager should always be sought first and language should always be appropriate and professional.

Mobile phones and electronic devices

- We advise against bringing mobile phones to school. If students do bring them, mobile phones and other electronic devices must not be seen or heard during the school day or on the site at any time. The sending of abusive or inappropriate text messages or files by Bluetooth or any other means is forbidden and will be dealt with in accordance with the school's behaviour and preventing and responding to bullying policies;
- Students are not permitted to use the cameras in their mobile phones at any time;
- Staff will be issued with a school mobile phone where contact with students is necessary;
- iPads provided to staff must be used in accordance with the school Acceptable Use policy both within school and outside;

- iPads provided to staff are done so to be used for work/educational purposes only and thus all apps installed should be appropriate for use in school;
- iPads for students should go through the school's web filtering so as to monitor use and help prevent students accessing inappropriate material;
- Where photos are to be taken of activities involving students a school issued technology should be used rather than personal technology;

Filtering
- The School will work in partnership with parents/carers, the DfE, partners and the Internet Service Provider to ensure that systems to protect students and staff are reviewed and improved regularly;
- If staff or students discover unsuitable sites, the URL and content must be reported to the ICT Technician and Senior member of staff;
- Any material the School deems to be unsuitable or illegal will be immediately referred to the Internet Watch Foundation (www.iwm.org.uk);
- Regular checks by Senior Staff will ensure that the filtering methods selected are appropriate, effective and reasonable;
- Filtering methods will be age and curriculum appropriate.

Authorising internet access
- All staff must read and sign a copy of the Safe Working Practice Agreement Safeguarding Students and Young People and the school's 'Acceptable Use of ICT Resources' document before using any School ICT resources.
- Any staff not directly employed by the school will be given a restricted internet access from the school site via a guest SSID which will be provided by the IT Team;
- The School will maintain a current record of all staff and students who are allowed access to the school's ICT systems.
- The school will maintain a record of students whose parents/carers have specifically requested that their child be denied internet or e-mail access;
- Parents/carers will be asked to sign and return the school's form stating that they have read and understood the School's 'Acceptable Use' document and give permission for their child to access ICT resources;
- Staff will supervise access to the internet from the school site for all students.

Backups and Anti-Virus
- All content that is saved to a shared or personal drive located on a server is backed up to a local server regularly;
- The local backup server regularly replicates backups to a secure data centre hosted by European Electronique;
- All computers in the school have an antivirus program with real time scanning installed to prevent any damage or data loss caused by malicious files or programs;
- Any USB memory drive/storage device should only be used for backup purposes, and need to be scanned by the IT Department before use. All files need to be uploaded to Google Drive instead of using USB Memory drives/storage devices.

Assessing risks
Emerging technologies offer the potential to develop teaching and learning tools but need to be evaluated to assess risks, establish the benefits and to develop good practice. The senior leadership team should be aware that technologies such as mobile phones with wireless internet access can bypass school filtering systems and allow a new route to undesirable material and communications.

In common with other media such as magazines, books and video, some material available through the Internet is unsuitable for students. The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of Internet content, it is

not always possible to guarantee that unsuitable material may never appear on a school computer. The school cannot accept liability for the material accessed, or any consequences of Internet access.

Emerging technologies will be examined for educational use and a risk assessment will be carried out before use in School is allowed and methods to identify, assess and minimise risks will be reviewed regularly. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Criminal Misuse Act 1990 and will be dealt with accordingly.

The Headteacher will ensure that the E-Safety Policy is implemented and compliance with the policy is monitored. Access to any websites involving gambling, games or financial scams is strictly forbidden and will be dealt with accordingly.

Rules for Internet access will be posted in all rooms where computers are used. Responsible Internet use, covering both school and home use, will be included in the curriculum. Students will be instructed in responsible and safe use before being allowed access to the Internet and will be reminded of the rules and risks before any lesson using the Internet. Students will be informed that internet use will be closely monitored and that misuse will be dealt with appropriately.

Consulting staff
It is essential that teachers and other adults working at the school are confident about using the internet in their work and should be given opportunities to discuss issues and develop appropriate teaching strategies. All staff are governed by the terms of this policy and will be provided with a copy and its importance explained. All new staff will be given access to a copy of the policy during their induction. Staff development in safe and responsible use of the internet will be provided as required. Staff will be aware that internet use will be monitored and traced to the original user. Discretion and professional conduct is essential. Senior managers will supervise members of staff who operate the monitoring procedures.

Maintaining ICT security
Personal data sent over the network will be encrypted or otherwise secured. Unapproved system utilities and executable files will not be allowed in students' work areas or attached to emails. The ICT technician will ensure that the system has the capacity to deal with increased traffic caused by Internet use.

Parents/carers and students will work in partnership with the school staff to resolve any issues. As with issues to do with substance misuse, there may be occasions when the school must contact the police. If appropriate, early contact should be made to discuss strategies and preserve possible evidence.

Sanctions for misuse may include any or all of the following:
- Interview/counselling by an appropriate member of staff;
- Informing parents/carers;
- Removal of internet access for a specified period of time, which may ultimately prevent access to files held on the system, including examination coursework;
- Exclusion;
- Referral to the police.

Monitoring, evaluation and review

The headteacher and Head of IT with the help of the Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every 2 years.

The governing board is responsible for approving this policy.

Head of ICT

March 2023