Head Teacher: Kirsten MacLeod

ICT, AI and Acceptable Use Policy

Version	Date	Amendment Details
	Approved date	Review date
1.0	Autumn 2023	Autumn 2025
2.0	Autumn 2025	Autumn 2027
3.0	Autumn 2026	Autumn 2027

Policy approved by Head Teacher: Autumn 202
Policy update: **Autumn 2026**
Policy to be reviewed again: **Autumn 2027**

Contents

- **1 Introduction and aims**
- **2 Relevant legislation and guidance**
- **3 Definitions**
- **4 Unacceptable use**
    a. 4.1 Exceptions from unacceptable use
    b. 4.2 Sanctions
- **5 Acceptable Use of Artificial Intelligence (AI)**
    - 5.1 Guiding Principles for Technology and AI Use
    - 5.2 Permitted Uses of AI by Staff
    - 5.3 Prohibited AI Uses & Academic Integrity (Pupils)
    - 5.4 Approved AI Tools
    - 5.5 Use of AI for Recording and Transcribing Meetings
    - 5.6 Ethical Considerations and Misuse Mitigation
- **6 Staff (including governors, volunteers, and contractors)**
    - 6.1 Access to school ICT facilities and materials
    - 6.1.1 Use of phones and email
    - 6.2 Personal use
    - 6.2.1 Personal social media accounts
    - 6.3 Remote access
    - 6.4 School social media accounts
    - 6.5 Monitoring and filtering of the school network and use of ICT facilities
- **7 Pupils**
    a. 7.1 Access to ICT facilities
    b. 7.2 Search and deletion
    c. 7.3 Unacceptable use of ICT and the internet outside of school
- **8 Parents/carers**
    a. 8.1 Access to ICT facilities and materials
    b. 8.2 Communicating with or about the school online
    c. 8.3 Communicating with parents/carers about pupil activity
- **9 Data security**
    a. 9.1 Passwords
    b. 9.2 Software updates, firewalls and anti-virus software
    c. 9.3 Data protection
    d. 9.4 Access to facilities and materials
    e. 9.5 Encryption
    f. 9.6 Data Protection Impact Assessments (DPIA) for AI
- **10 Protection from cyber attacks**
- **11 Internet access**
    - 11.1 Pupils
    - 11.2 Parents/carers and visitors
- **12 Monitoring and review**
- **13 Related policies**

1 Introduction and aims

Information and communications technology (ICT) and Artificial Intelligence (AI) are integral parts of the way Newham Pupil Referral Units (PRUs) work, and serve as critical resources for pupils, staff (including the senior leadership team), governors, management committee members, volunteers and visitors. ICT and AI support teaching and learning, student well-being, pastoral care, and administrative functions across our school.

However, the ICT resources, digital platforms, and AI facilities our school uses could also pose risks to data protection, online safety, academic integrity, and safeguarding.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources and AI tools for staff, pupils, parents/carers and governors
- Promote student well-being and maintain human interaction at the core of our educational practice, ensuring technology and AI supplement rather than replace the crucial relationship between dedicated staff and pupils
- 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 (UK GDPR), online safety and safeguarding, both on and off the premises
- Outline clear boundaries of acceptable behavior to mitigate the risk of inappropriate communication taking place between staff and pupils and avoid misplaced allegations
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of ICT systems and AI technologies
- Support the school in teaching pupils safe, responsible, ethical, and effective internet, ICT, and AI use

This policy covers all users of our school's ICT facilities and AI systems, including governors, staff, pupils, volunteers, contractors and visitors, whether using school-provided equipment or personal devices for work-related purposes.

Breaches of this policy may be dealt with under our staff code of conduct, staff discipline policy, or pupil behavior policy.

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)
- 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 (KCSIE)
- 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

- Department for Education (DfE) Statement on Generative Artificial Intelligence in Education
- Joint Council for Qualifications (JCQ) guidance on AI use in assessments

3 Definitions

- **ICT facilities:** all facilities, systems and services including, but not limited to, network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, virtual learning environments (VLEs), 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 ICT service.
- **Artificial Intelligence (AI) & Generative AI:** technology, algorithms, or automated platforms that can create new content (such as text, images, audio, video simulations, or code) or analyse complex data based on models trained on large volumes of information (e.g. large language models like Google Gemini, transcription platforms, and AI embedded in MIS systems).
- **Users:** anyone authorised by the school to use the school's ICT facilities or AI tools, 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, AI oversight, and/or monitoring of the ICT facilities.
- **Materials:** files and data created using the school's ICT facilities or AI tools including but not limited to documents, photos, audio, video, transcriptions, printed output, web pages, social networking sites and blogs.

4 Unacceptable use

The following is considered unacceptable use of the school's ICT facilities and AI tools. Any breach of this policy may result in disciplinary or behaviour proceedings.
Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities or AI tools 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
- 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
- Using AI tools to generate deepfakes, synthetic media, or impersonation materials
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing, or removing from its location, confidential information about the school, its pupils, or other members of the school community
- Inputting sensitive personal data (e.g. health information, religious beliefs, or biometric data) into unapproved public AI tools
- 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 programme, tool or item of

software designed to interfere with the functioning of the school's ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to the school's ICT facilities
- Removing, deleting or disposing of the school's ICT 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
- Using AI tools and generative chatbots (such as Google Gemini, ChatGPT, etc.):
    - During internal and external qualification assessments, NEAs, and coursework where it violates JCQ guidelines
    - To write homework or class assignments where AI-generated content is presented as a pupil's own independent work

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or relevant designated staff 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 ICT facilities.

4.1 Exceptions from unacceptable use

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

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 staff discipline, staff code of conduct, and pupil behaviour policy.

5 Acceptable Use of Artificial Intelligence (AI)

5.1 Guiding Principles for Technology and AI Use

Our approach to AI is guided by our core values of kindness, courage, and resilience:

- **Student Well-being & Human Interaction:** Technology and AI must supplement and support our teaching—not replace it. AI must not replace the crucial relationship between dedicated staff and pupils.
- **Ethical Use:** AI must be used in a fair, transparent, and non-discriminatory manner. Potential algorithmic biases must be recognised and mitigated.

- **Data Privacy & Security:** Student data must be protected in accordance with UK GDPR. Clear protocols for data collection, storage, and usage must be followed. No sensitive personal data may be entered into public AI tools.
- **Safeguarding:** All AI tools must be vetted for potential risks to avoid compromising student safety.
- **Transparency & Accountability:** Stakeholders must understand when AI is being used. Human judgement remains at the heart of our decision-making ("human in the loop").

5.2 Permitted Uses of AI by Staff

Staff are permitted to explore and utilise school-approved AI tools to assist in managing their work, ensuring outputs complement their professional judgment and expertise. Approved uses include:

- Personalised learning support, adaptive tasks, extension work, and scaffolding
- Assisting with lesson planning, curriculum ideas, and alternative topic explanations
- Gathering insights and analysing datasets for pupil attainment, attendance, and behavioural patterns to support early intervention
- Automating aspects of objective marking and drafting feedback
- Assisting in drafting pupil reports, administrative tasks, scheduling, and meeting communications (staff must review and modify AI outputs to ensure they reflect personal observations and accurate assessments)
- Recording and transcribing meetings in accordance with Section 5.5

5.3 Prohibited AI Uses & Academic Integrity (Pupils)

- **Direct Pupil Access Prohibited:** At this time, pupils are not permitted to have direct access to Gemini or any other Generative AI platform within lessons. Staff are responsible for monitoring pupils to ensure this is enforced until full tracking, monitoring, and safeguarding systems are established.
- **Academic Integrity & JCQ Regulations:** In accordance with JCQ regulations, all work submitted for qualification assessments (including NEAs and coursework) must be a student's own independent work. Copying or paraphrasing AI-generated text, calculations, or analysis and submitting it as one's own constitutes malpractice.
- **Acknowledging AI Research:** Where explicitly permitted as a research source, AI usage must be fully acknowledged, detailing the name of the tool, date generated, and the prompt/output details.

5.4 Approved AI Tools

Staff may only use AI tools that have been vetted and authorised by Newham PRUs:

- **Google Gemini** (accessed strictly through official school work login)
- **Formally approved third-party applications with integrated AI** (including CPOMS, BROMCOM, and Canva)

5.5 Use of AI for Recording and Transcribing Meetings

1. All participants must be informed in advance if a meeting will be recorded and transcribed using AI tools, and explicit consent must be obtained.
2. Recordings and transcriptions must only capture necessary meeting content. Private conversations outside agenda items must not be recorded.
3. Transcriptions and AI draft notes must be stored securely and deleted once official minutes are approved and ratified.

4. Draft minutes produced by AI must be reviewed and validated by a human before circulation. AI must not be used to independently interpret sensitive discussions (e.g. disciplinary or safeguarding meetings) without human oversight.

5.6 Ethical Considerations and Misuse Mitigation

When using AI systems, staff must maintain awareness of three primary limitations:

- **Bias:** AI models reflect biases present in training data, which could generate discriminatory output.
- **Accuracy:** Information generated by AI can be incorrect or hallucinated. All content must be fact-checked by staff.
- **Currency:** AI models may not reflect real-time or recent information updates.

6 Staff (including governors, volunteers, and contractors)

6.1 Access to school ICT facilities and materials

The IT Manager / School Business Manager manages access to the school's ICT facilities and materials for staff, including computers, tablets, mobile phones, and access permissions for programmes and files.
Staff will be provided with unique login/account information and passwords that they must use when accessing ICT facilities. Staff must not share their login details.

6.1.1 Use of phones and email

The school provides each member of staff with an email address for work purposes only. Multi-factor authentication (MFA) must be enabled. All work-related business must be conducted using this account and not personal email addresses.
Staff must not share personal email addresses or phone numbers with parents/carers or pupils. School-provided mobile devices must be used for work tasks unless express, time-limited permission to use a personal device is granted by the Headteacher and IT department.
Staff must take extra care when sending sensitive or confidential information by email. Attachments containing sensitive data should be encrypted, shared via secure links, or password-protected. Email errors containing personal data must be reported immediately to the internal Data Protection Lead.

6.2 Personal use

Staff are permitted to occasionally use school ICT facilities for personal use outside of teaching/contact time, provided such use does not constitute unacceptable use, take place in the presence of pupils, or interfere with job duties. Staff may not store personal media files (music, photos, videos) on school ICT facilities.

6.2.1 Personal social media accounts

Members of staff must ensure their use of personal social media is appropriate at all times and maintains professional boundaries with pupils and parents/carers.

6.3 Remote access

Remote access to school systems is cloud-based or conducted via Virtual Private Networks (VPNs). Staff accessing school facilities or data remotely must abide by all policy rules and are only permitted to use personal devices where express, time-limited authorisation has been granted by the Headteacher and IT department.

Where staff are authorised to use a personal device (such as a shared home computer) for remote access, they must ensure that:

- The device has active, up-to-date anti-virus and anti-malware software installed, alongside a functioning firewall and regular operating system security updates.
- They use a unique, private user account and strong password that is strictly separate from any other members of their household or other users who share the device.
- Passwords and login credentials for school systems are not saved onto shared web browsers, unapproved password managers, or device keychains.
- They do not access school systems or data from public computers or unsecured public Wi-Fi hotspots.
- Non-cloud school software is not downloaded onto personal or shared home devices without the express permission of the Headteacher.

6.4 School social media accounts

Official social media accounts are managed by authorised personnel only. Unauthorised staff must not attempt to access or post to official school accounts.

6.5 Monitoring and filtering of the school network and use of ICT facilities

To safeguard pupils and promote welfare, the school filters and monitors internet sites, email accounts, bandwidth usage, phone calls, and user activity logs. Filtering and monitoring are managed by authorised IT personnel in coordination with the Designated Safeguarding Lead (DSL) and Governing Board in compliance with DfE standards.

7 Pupils

7.1 Access to ICT facilities

Computers and equipment in school's classrooms are available to pupils only under the direct supervision of staff.

7.2 Search and deletion

Under the Education Act 2011 and KCSIE guidelines, the Headteacher and authorised staff may search pupil devices and confiscate electronic devices if there are reasonable grounds for suspecting the device contains banned items, offensive material, or evidence relating to an offence. If images or files are suspected to be indecent images of children (nude/semi-nude images), staff will not view, print, or save the file, but will immediately confiscate the device and report to the DSL.

7.3 Unacceptable use of ICT and the internet outside of school

The school may sanction pupils if they engage in unacceptable ICT use outside of school premises that impacts the safety of the school community, defames the school, or violates the behaviour

policy.

8 Parents/carers

8.1 Access to ICT facilities and materials

Parents/carers do not have routine access to school ICT facilities unless working in an official volunteer capacity, in which case staff policy rules apply.

8.2 Communicating with or about the school online

Parents/carers are expected to model respectful online communication when interacting with or commenting about the school online.

8.3 Communicating with parents/carers about pupil activity

The school will inform parents/carers about online platforms pupils are required to use for educational tasks and homework.

9 Data security

The school maintains technical security measures including firewalls, multi-factor authentication, user permissions, and anti-malware software to safeguard user accounts and data.

9.1 Passwords

Users must set strong passwords and keep them secure. Staff must use the required password manager to store credentials securely.

9.2 Software updates, firewalls and anti-virus software

All school devices will have automatic security updates and anti-virus protection configured. Any authorised personal devices used to access the school network or school data remotely must also maintain active, up-to-date anti-virus, anti-malware, and firewall protections. Users must not attempt to bypass administrative safeguards..

9.3 Data protection

All personal data must be processed in compliance with UK GDPR and the school's Data Protection Policy.

9.4 Access to facilities and materials

Access permissions are managed based on job roles. Users must log out of systems and lock equipment when unattended.

9.5 Encryption

School devices containing sensitive or personal data are appropriately encrypted.

9.6 Data Protection Impact Assessments (DPIA) for AI

Before introducing new AI tools, a DPIA must be conducted with the Data Protection Officer to assess data processing scope, alternatives, algorithmic accuracy, bias, safety safeguards, and ensure pupil data is not used to train public models.

10 Protection from cyber attacks

The school implements multi-layered security controls, conducts regular data backups, provides staff cyber-security training, and maintains an incident response plan. The school will not engage in ransom payments in the event of ransomware attacks.

11 Internet access

The school's wireless internet connection is secure and filtered.

11.1 Pupils

Pupils may access the Wi-Fi network only for educational tasks under staff supervision.

11.2 Parents/carers and visitors

Visitors and parents may only access guest Wi-Fi when authorised by the Headteacher for official visits.

12 Monitoring and review

An AI Steering Group and AI Community of Practice will assist in monitoring technology adoption. The Headteacher, IT Lead, and School Business Manager monitor implementation. This policy will be formally reviewed every 24 months (Autumn 2028) by the Governing Board.

13 Related policies

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

- Online safety
- Social media
- Safeguarding and child protection
- Behaviour policy
- Staff discipline and Staff code of conduct
- Data protection & DPIA procedure
- IT Disaster Recovery
- Curriculum Policy (Whole School and EYFS)