NEW AVENUE SCHOOL

| | |
|---|---|
| Policy Name | ICT and Acceptable Use |
| Policy No. | NA32 |
| Date Written | 12.07.24 |
| Date to Review | 12.07.26 |
| Author | Anthony Merriman |
| Cross Reference | • Child Protection Policy<br>• Curriculum Policy<br>• Pupil Assessment Policy<br>• SEND Policy<br>• ICT and Acceptable Use Policy |

Contents

## 1. Aims

ICT is a core learning and operational resource at New Avenue School. This policy sets clear expectations for staff, pupils, governors, parents, and visitors in using ICT safely, lawfully, and responsibly. It ensures compliance with statutory safeguarding duties and supports our SEMH context.

The aims are to:

- Safeguard pupils by embedding **safe and effective use of ICT**.
- Provide a framework for the **responsible use of devices, networks, and online platforms**.
- Set out how the school meets the **DfE Filtering & Monitoring Standards**.
- Support compliance with **KCSIE 2025**, the **Independent School Standards (2025)**, and the **Data Protection and Digital Information Act 2025**.

## 2. Legislation and Guidance

This policy reflects and complies with:

- Keeping Children Safe in Education 2025
- Working Together to Safeguard Children 2023
- Education (Independent School Standards) 2025
- Education (Pupil Registration) Regulations 2006 (amended 2024)
- Data Protection Act 2018 / UK GDPR / Data Protection and Digital Information Act 2025
- DfE Filtering & Monitoring Standards (2023, refreshed 2025)
- UKCIS Guidance: Sharing Nudes and Semi-Nudes
- Searching, Screening and Confiscation Guidance 2022
- Computer Misuse Act 1990
- Human Rights Act 1998

## 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, websites, web applications, or services.
- **Users:** Anyone authorised by the school to use the school's 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 agreed by an authorised user.
- **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 school's ICT facilities, including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.

## 4. Unacceptable use

Unacceptable use of the school's ICT facilities will include but not be limited to:

- 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 will be 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 that will defame or disparage 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.
- 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.
- 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 will be radicalised, extremist, racist, antisemitic, or discriminatory in any other way.
- Using AI tools and generative chatbots (such as ChatGPT and Google Bard) during assessments, to write homework or class assignments where AI-generated text or imagery will be presented as their own work.
- Circumventing, disabling, or testing the school's filtering and monitoring systems.
- Accessing or promoting misinformation, disinformation, conspiracy theories, extremist or radicalising content.
- Using AI tools (e.g. ChatGPT, image generators) in ways that:
  - Bypass academic integrity (e.g. submitting AI-generated work as original).
  - Generate harmful, discriminatory, or unsafe material.
  - Process or expose personal/safeguarding data.
  - Recording, sharing, or streaming content that breaches safeguarding, privacy, or consent.

- Any use that increases the **safeguarding risk to pupils with EBSA or anxiety** (e.g. coercive group chats, online bullying).

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

## 5. Staff

### 5.1 Access to School ICT Facilities and Materials

The school's computer science lead, in liaison with PSD Group, will manage access to the school's ICT facilities and materials for staff. That includes but is not limited to:

- Computers, tablets, mobile phones, and other devices.
- Access permissions for programmes, files, and safeguarding systems.

Staff will be provided with unique login/account information and passwords that they must use when accessing school ICT facilities. **All staff accounts must use multi-factor authentication (MFA) where available.** Staff who need permissions updated must contact the ICT manager.

### 5.1.1 Use of Phones and Email

- The school will provide each staff member with a work email account. This account must be used for all work communication.
- Staff must not use personal email or personal phone numbers with pupils or parents/carers.
- **All work email accounts must have MFA enabled.**
- Sensitive or confidential information must only be sent via encrypted attachments.
- Data breaches (e.g. mis-sent emails) must be reported immediately to the ICT manager and DSL, following the school's Data Breach Procedure.

### 5.2 Personal Use

- Occasional personal use of school ICT facilities is permitted outside contact/teaching time, provided it does not breach Section 4 (Unacceptable Use).
- Staff must not store personal media (music, photos, videos) on school systems.
- **Personal use remains subject to filtering and monitoring under the DfE Standards (2023, updated 2025).**
- Staff may use personal devices in line with the Mobile Phone/Personal Device Policy, but must never access or process safeguarding data on personal devices unless specifically authorised by the Headteacher and risk-assessed.

### 5.2.1 Personal Social Media Accounts

- Staff must set appropriate security on personal social media accounts.
- Staff must not interact with pupils or parents/carers through personal social media.
- **Staff must not post content that undermines the school's safeguarding duties or compromises their professional integrity.**

### 5.3 School Social Media Accounts

- The school currently maintains a LinkedIn account managed by designated staff.
- Only authorised staff may post on school accounts.
- Content must be respectful, accurate, and never disclose personal/safeguarding data.

### 5.4 Monitoring and Filtering of the School Network and Use of ICT Facilities

To safeguard pupils and comply with **KCSIE 2025** and the **DfE Filtering & Monitoring Standards**, the school reserves the right to filter and monitor all use of ICT facilities. This includes:

- Internet sites visited
- Bandwidth usage
- Email traffic
- User activity logs
- Any electronic communication on school systems

**Roles and Responsibilities:**

- **Governors**: hold strategic oversight and review filtering/monitoring reports termly.
- **DSL**: leads on interpreting filtering/monitoring alerts for safeguarding purposes, escalating where pupils may be at risk (including EBSA-related online risks such as coercive group chats, online bullying, or harmful content).
- **ICT Lead/Oakford Technology**: manage technical setup, carry out system testing, report results to SLT and governors.
- **All Staff**: must report any online concerns flagged by monitoring to the DSL.

**Annual Online-Safety Risk Assessment**

- The school carries out an annual risk assessment of its filtering and monitoring systems, covering:
  - Safeguarding risks (e.g. harmful content, online grooming, mis/disinformation).
  - Technical vulnerabilities (e.g. attempts to bypass filters).
  - Risks linked to pupil need (e.g. EBSA/anxiety exacerbated by online conflict).
- Findings are shared with governors and minuted.

## 6. Pupils

**6.1 Access to ICT Facilities**

- Pupils will be given access to ICT facilities (computers, laptops, tablets, internet) during structured lessons, supervised activities, and agreed times for independent work.
- Access may be restricted where misuse occurs.
- **Access arrangements for pupils with high levels of anxiety or EBSA will be personalised, with phased introductions to ICT systems if needed.**
- **All pupil accounts are subject to monitoring and filtering, in line with DfE Standards.**

**6.2 Search and Deletion**

Under the Education Act 2011, the headteacher and authorised staff may search pupils and confiscate devices where there are reasonable grounds to suspect:

- The device poses a risk to staff or pupils.
- The device is listed as a banned item in school rules.
- The device may provide evidence relating to an offence.

This includes but is not limited to:

- Pornography
- Abusive or threatening messages, images, or videos
- Indecent images of children
- Material linked to criminal or extremist activity
- **Misinformation, disinformation, conspiracy theories, or harmful online challenges that present safeguarding risks**

Before a search, staff will:

- Assess urgency and risks to safety.
- Explain reasons to the pupil and seek cooperation.
- Involve the DSL where safeguarding concerns exist.

If inappropriate or illegal material is found:

- The DSL will be informed immediately.
- If material may constitute criminal evidence, the device will be passed to police without deletion.
- **If indecent images of a child are suspected, staff will not view or share the material but will follow the school's Safeguarding Policy and UKCIS guidance.**

**6.3 Unacceptable Use of ICT and the Internet (In and Outside of School)**

The school will sanction pupils in line with the Behaviour Policy for unacceptable ICT use, even if outside school premises. This includes:

- Breaching intellectual property or copyright.
- Bullying, harassment, or unlawful discrimination online.
- Accessing, creating, or sharing pornographic, offensive, extremist, or harmful material.
- **Engaging with or spreading misinformation, disinformation, or conspiracy theories.**
- Consensual or non-consensual sharing of nude or semi-nude images or livestreams.
- Defaming or bringing the school into disrepute online.

- Sharing confidential information about the school, staff, or pupils.
- Attempting unauthorised access to systems or restricted data.
- Causing intentional damage to ICT facilities or data.
- **Using AI tools (text, image, or video generators) to:**
  - Submit work dishonestly as their own.
  - Create harmful, discriminatory, or unsafe content.
  - **Manipulate or share content that could heighten anxiety, avoidance behaviours, or safeguarding risks for EBSA pupils.**
- Using language online that is offensive, threatening, or discriminatory.

### 6.4 Online Safety Education

- Pupils will be explicitly taught how to recognise, manage, and report online risks, including harmful challenges, grooming, radicalisation, and misinformation.
- **Lessons will be designed with EBSA-sensitive practice in mind, ensuring gradual exposure and building confidence in safe ICT use.**
- The DSL will ensure online safety is integrated into the PSHE curriculum, Computing lessons, and safeguarding briefings.

## 7. Parents/carers

### 7.1 Access to ICT Facilities and Materials

- Parents/carers will not normally have access to the school's ICT facilities.
- Where parents/carers are working with the school in an official capacity, access may be granted at the Headteacher's discretion.
- **Any such access must be risk-assessed, logged, and restricted to the minimum necessary. Parents granted access must comply with this Acceptable Use Policy.**

### 7.2 Communicating with or about the School Online

- Parents/carers are expected to model respectful and safe online behaviour at all times.
- Parents/carers must not post content that is defamatory, threatening, discriminatory, or breaches the privacy of pupils, staff, or families.
- **Parents must not use online platforms to share misinformation, disinformation, conspiracy theories, or harmful content relating to the school.**
- Concerns should always be raised directly with the school and not through public online forums.

### 7.3 Communicating with Parents/Carers about Pupil Activity

The school will keep parents informed about their child's online activity in school, including:

- The websites, platforms, or tools pupils are asked to use for homework or projects.
- The nature and purpose of any online interactions between staff and pupils (e.g. through Teams, email, or managed platforms).
- **When AI tools are used in teaching or learning, parents will be informed of the purpose, boundaries, and safeguards in place.**
- **Parents will also be updated on filtering and monitoring arrangements so they understand how inappropriate or harmful content is blocked and flagged.**

### 7.4 Partnership in Online Safety

- Parents are key partners in helping pupils stay safe online. The school will:
  - Share regular updates on online safety risks through newsletters, workshops, and briefings.
  - Provide guidance for supporting children with high anxiety or EBSA in managing safe online routines at home.
  - Encourage parents to use parental controls, filtering, and device monitoring at home.
- **Parents are expected to reinforce safe ICT habits outside school and to work with the school and DSL where safeguarding concerns arise.**

## 8. Data Security

The school is responsible for making sure it has robust security protections and procedures in place to safeguard its systems, staff, and pupils. This includes protecting ICT resources, user accounts, and personal data. Procedures are regularly reviewed to keep pace with evolving cybercrime threats and new statutory requirements.

All staff, pupils, parents/carers, and others who use the school's ICT facilities must follow safe computing practices at all times. The school will aim to meet the cyber security standards recommended by the DfE's guidance on **Digital and Technology Standards in Schools and Colleges**.

### 8.1 Passwords

- All users must create strong, unique passwords.
- Passwords must never be shared.
- **All staff accounts and high-level pupil accounts must use multi-factor authentication (MFA).**
- Users are responsible for securing any accounts or files they control.

### 8.2 Software Updates, Firewalls, and Anti-Virus

- All school ICT devices must have firewalls, anti-virus software, and automatic security updates enabled.
- Updates must be installed promptly, with critical patches applied immediately.

### 8.3 Data Protection

- All personal data will be processed and stored in line with the **UK GDPR**, **Data Protection Act 2018**, and the **Data Protection and Digital Information Act 2025 (DUAA 2025)**.
- **The school's Record of Processing Activity (RoPA) will include filtering/monitoring logs, safeguarding platforms, and AI-assisted tools.**
- **Safeguarding and attendance-related data, including EBSA phased attendance plans, will be stored securely and shared only with authorised professionals.**
- Any data breach must be reported immediately to the Data Protection Officer (DPO) and DSL.

### 8.4 Access to Facilities and Materials

- User access rights are defined by role and managed by the ICT lead.
- **Least-privilege access** principles apply: users are only granted access to systems or files needed for their role.
- **Access reviews are conducted termly to prevent privilege creep.**

### 8.5 Encryption and Remote Access

- All school devices and storage systems must have encryption enabled.
- Staff must only access school data remotely using school-authorised devices and the school's secure VPN.
- **Where personal devices are authorised, they must be risk-assessed, encrypted, and protected with MFA.**

### 8.6 Filtering, Monitoring and AI Data

- Filtering and monitoring systems generate data logs that may include user activity, flagged searches, or access attempts.
- **These logs are processed under the school's lawful safeguarding duty (KCSIE 2025) and mapped in the RoPA.**
- **AI tools used for teaching or administration must never process safeguarding, sensitive, or personal data unless explicitly risk-assessed and approved by the Headteacher and DPO.**

## 9. Protection from Cyber Attacks

The school recognises that cyber security is a safeguarding responsibility. A successful attack could compromise personal data, disrupt learning, or expose pupils to harm. We therefore treat cyber security as a priority, with proportionate, layered defences.

The school will:

- Work with Oakford Technology to make sure cyber security is given appropriate time, expertise, and resources.
- Provide **annual staff training on cyber security, phishing awareness, and secure use of AI tools**.
- Make sure staff are aware of reporting and incident-response procedures.

- Put **multi-layered technical controls** in place, including firewalls, endpoint protection, and secure configurations.
- **Carry out annual penetration testing and vulnerability scans**, reporting findings to governors.
- **Test filtering and monitoring systems regularly** to check effectiveness, as required by the DfE Standards.
- Back up critical data daily, with secure off-site/cloud storage and recovery testing.
- Delegate specific responsibility for maintaining the security of the MIS and other critical systems to the ICT manager.
- Require staff to access the school network remotely only via VPN, with MFA enabled.
- Store all passwords securely using an encrypted password manager.
- **Undertake supply chain checks** to confirm that third-party providers (including EdTech, AI, and safeguarding platforms) have appropriate security and data protection measures.
- Maintain a firewall that is active and reviewed regularly.
- **Run simulated phishing exercises** at least annually to test staff awareness.
- **Escalate serious cyber incidents to the DPO, DSL, and (if necessary) the ICO and National Cyber Security Centre (NCSC).**

## 10. Internet access

The school's wireless internet connection is secure, filtered, and monitored in line with statutory safeguarding duties. Access to the internet is a privilege, not a right, and must always be consistent with the aims of this policy.

### 10.1 Pupils

- Pupils will have supervised access to the internet through school devices, subject to age, need, and curriculum requirements.
- **All pupil activity is filtered and monitored in real time**, with alerts escalated to the DSL when safeguarding risks are identified.
- **Filtering actively blocks extremist, pornographic, gambling, radicalising, mis/disinformation, and conspiracy-related content.**
- **EBSA-sensitive arrangements** may include phased or restricted access to online platforms to reduce anxiety or avoidance triggers.
- Pupils are taught explicitly how to use the internet safely and responsibly through PSHE, Computing, and pastoral programmes.
- Attempts to bypass filters or monitoring will be treated as a serious breach of this policy and sanctioned under the Behaviour Policy.

### 10.2 Parents/Carers and Visitors

- Parents/carers and visitors will not normally be permitted to use the school's WiFi.
- Where authorisation is granted by the Headteacher, access will be restricted, time-limited, and monitored.
- **Guest access will always be on a separate network from pupil and staff systems.**
- Visitors must never attempt to connect unauthorised devices to the school network.

### 10.3 Filtering and Monitoring Standards

- The school meets the **DfE Filtering and Monitoring Standards (2025)** by ensuring:
  - Filtering and monitoring are age-appropriate, responsive, and regularly tested.
  - The governing body reviews filtering/monitoring reports at least termly.
  - The DSL has lead responsibility for interpreting alerts and escalating safeguarding concerns.
  - Technical testing and reports are managed by the ICT lead and Oakford Technology.
  - An **annual risk assessment** of filtering/monitoring effectiveness is completed and shared with governors.

## 11. Monitoring and Evaluation

- The Headteacher and Computer Science Lead, in liaison with Oakford Technology, will monitor the implementation of this policy.
- The policy will be **reviewed annually, or sooner if statutory guidance changes** (e.g. updates to KCSIE, ISS, DfE standards, or data protection law).

### 11.1 Oversight and Governance

- The **governing body** receives termly reports on ICT usage, filtering/monitoring effectiveness, and safeguarding alerts.
- Governors ensure compliance with the **DfE Filtering and Monitoring Standards** and review the school's **annual online-safety risk assessment**.
- Minutes of governor meetings will record scrutiny of filtering/monitoring arrangements and cyber security.

### 11.2 Safeguarding Monitoring

- The **DSL has lead responsibility** for understanding and interpreting filtering/monitoring systems.
- Alerts flagged by the system (e.g. attempts to access harmful content, evidence of online bullying, signs of grooming, or EBSA-related online triggers) are reviewed daily by the DSL or deputy.
- Safeguarding concerns are escalated in line with the Child Protection and Safeguarding Policy.

### 11.3 Technical Monitoring

- The **ICT lead and Oakford Technology** carry out regular technical checks and penetration testing.
- Filtering and monitoring systems are **tested at least termly** to ensure they remain effective and age-appropriate.
- Results of these tests are logged and reported to SLT and governors.

### 11.4 Evaluation of Impact

- The policy's effectiveness is evaluated by considering:
  - Compliance with statutory standards (KCSIE 2025, ISS 2025, DUAA 2025).
  - Evidence from safeguarding casework, including EBSA pupils' online risks.
  - Outcomes of staff and pupil online-safety training.
  - Technical performance data (blocked content, alerts, system uptime).
  - Feedback from pupils, staff, and parents on online-safety education and ICT provision.

### 11.5 Continuous Improvement

- The school commits to ongoing improvement of its ICT and online-safety practice.
- New and emerging risks (e.g. generative AI misuse, conspiracy-driven disinformation, evolving cyber threats) will be reviewed annually.
- Lessons learned from incidents or monitoring will inform future updates to this policy and staff training.

Updates

| Dates | Comments |
|---|---|
| 06.03.25 | Updated Social Media section to reflect current presence of school. |
| 16.09.25 | Updated in line with KCSIE 2025 and other regulatory updates. |
| | |