NEW AVENUE
SCHOOL

Policy Name	ICT and Acceptable Use
Policy No.	NA32
Date Written	12.07.24
Date to Review	12.07.25
Author	Anthony Merriman
Cross Reference	• Child Protection Policy • Curriculum Policy • Pupil Assessment Policy • SEND Policy • ICT and Acceptable Use Policy

Contents

1. Aims

Information and communications technology (ICT) will be an integral part of the way our school works and will be a critical resource for pupils, staff (including the senior leadership team), governors, volunteers, and visitors. It will support teaching and learning as well as the pastoral and administrative functions of the school. However, the ICT resources and facilities our school uses could also pose risks to data protection, online safety, and safeguarding.

This policy will aim to:

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

This policy will cover 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 disciplinary policy, behaviour policy, staff discipline policy, or staff code of conduct.

2. Legislation and Guidance

This policy will refer to and comply 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 2023
- Searching, screening, and confiscation: advice for schools 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes

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.

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 school staff. That will include but not be limited to:

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

Staff will be provided with unique login/account information and passwords that they must use when accessing the school's ICT facilities. Staff who have access to files that they are not authorised to view or edit or who need their access permissions updated or changed should contact the ICT manager.

5.1.1 Use of Phones and Email

The school will provide each member of staff with an email address. This email account will be used for work purposes only. Staff will enable multi-factor authentication on their email account(s). All work-related business will be conducted using the email address the school has provided. Staff will not share their personal email addresses with parents/carers and pupils and will not send any work-related materials using their personal email account.

Staff will 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 will be 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 will not mean that an email cannot be recovered for the purposes of disclosure. All email messages will be treated as potentially retrievable.

Staff will take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information will be encrypted so that the information is only accessible by the intended recipient. If staff receive an email in error, the sender will be informed and the email deleted. If the email contains sensitive or confidential information, the user will not make use of that information or disclose that information.

If staff send an email in error that contains the personal information of another person, they will inform the ICT manager immediately and follow our data breach procedure.

Staff will not give their personal phone number(s) to parents/carers or pupils. Staff will use phones provided by the school to conduct all work-related business. School phones will not be used for personal matters. Staff who will be 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 will be permitted to occasionally use school ICT facilities for personal use, subject to certain conditions set out below. This permission will not be overused or abused. The ICT manager may withdraw or restrict this permission at any time and at their discretion. Personal use will be permitted provided that such use:

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

Staff will 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. Where breaches of this policy will be found, disciplinary action may be taken.

Staff will be permitted to use their personal devices (such as mobile phones or tablets) in line with the school's mobile phone/personal device policy. Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by putting personal details in the public domain where pupils and parents/carers could see them.

Staff will take care to follow the school's guidelines on use of social media and use of email to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal Social Media Accounts

Members of staff will make sure their use of social media, either for work or personal purposes, is appropriate at all times. The school will have guidelines for staff on appropriate security settings for Facebook accounts.

5.3 School Social Media Accounts

The school will have a LinkedIn account managed by designated staff. Staff members who will not be authorised to manage or post to the account must not access or attempt to access the account. The school will have guidelines for what may and must not be posted on its social media accounts. Those who will be authorised to manage or post to the account must make sure they abide by these guidelines at all times.

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

To safeguard and promote the welfare of children and provide them with a safe environment to learn, the school will reserve the right to filter and monitor the use of its ICT facilities and network. This will include but not be limited to the filtering and monitoring of:

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

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

The school will monitor 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.

Our governing board will be responsible for making sure that:

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

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

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

6. Pupils

6.1 Access to ICT Facilities

Explain which ICT facilities will be available to pupils, when, and under what circumstances.

6.2 Search and Deletion

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

- Poses a risk to staff or pupils.
- Is identified in the school rules as a banned item for which a search can be carried out.
- Is evidence in relation to an offence.

This will include but not be limited to:

- Pornography.
- Abusive messages, images, or videos.
- Indecent images of children.
- Evidence of suspected criminal behaviour.

Before a search, the authorised staff member will:

- Make an assessment of how urgent the search is and consider the risk to other pupils and staff. If the search is not urgent, they will seek advice from the headteacher or DSL.
- Explain to the pupil why they are being searched, how and where the search will happen, and give them the opportunity to ask questions about it.
- Seek the pupil's cooperation.

The authorised staff member will:

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

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

If inappropriate material is found on the device, it will be up to the staff member in conjunction with the DSL or headteacher to decide on a suitable response.

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

If a staff member suspects a device may contain an indecent image of a child, they will:

- Not view the image.
- Not copy, print, share, store, or save the image.
- Confiscate the device and report the incident to the DSL (or deputy) immediately.

Any searching of pupils will be carried out in line with the DfE's latest guidance on searching, screening, and confiscation.

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 making statements which are deemed to be advocating illegal activity.
- Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene, or otherwise inappropriate.

- Consensual or non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams.
- 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 the school's ICT facilities or materials.
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user and/or those they share it with are not supposed to have access or without authorisation.
- Using inappropriate or offensive language.

7. Parents/carers

7.1 Access to ICT Facilities and Materials

Parents/carers will not have access to the school's ICT facilities as a matter of course. However, parents/carers working for or with the school in an official capacity may be granted an appropriate level of access or be permitted to use the school's facilities at the headteacher's discretion.

Where parents/carers will be 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 will believe it is important to model for pupils and help them learn how to communicate respectfully with and about others online. Parents/carers will play a vital role in helping model this behaviour for their children, especially when communicating with the school through our website and social media channels.

7.3 Communicating with Parents/Carers about Pupil Activity

The school will ensure that parents and carers are made aware of any online activity that their children are being asked to carry out. When we will ask pupils to use websites or engage in online activity, we will communicate the details of this to parents/carers in the same way that information about homework tasks is shared.

In particular, staff will let parents/carers know which (if any) person or people from the school pupils will be interacting with online, including the purpose of the interaction.

8. Data Security

The school will be responsible for making sure it has the appropriate level of security protection and procedures in place to safeguard its systems, staff, and learners. It will take steps to protect the security of its computing resources, data, and user accounts. The effectiveness of these procedures will be reviewed periodically to keep up with evolving cybercrime technologies.

Staff, pupils, parents/carers, and others who use the school's ICT facilities will use safe computing practices at all times. We will aim to meet the cyber security standards recommended by the Department for Education's guidance on digital and technology standards in schools and colleges.

8.1 Passwords

All users of the school's ICT facilities will set strong passwords for their accounts and keep these passwords secure. Users will be responsible for the security of their passwords and accounts and for setting permissions for accounts and files they control.

8.2 Software Updates, Firewalls, and Anti-Virus Software

All of the school's ICT devices that will support software updates, security updates, and anti-virus products will have these installed and be configured to perform such updates regularly or automatically.

8.3 Data Protection

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

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 will be managed by the relevant person.

8.5 Encryption

The school will make sure that its devices and systems have an appropriate level of encryption.

School staff will only use personal devices to access school data, work remotely, or take personal data out of school if they have been specifically authorised to do so by the headteacher.

9. Protection from Cyber Attacks

The school will:

- Work with SchoolCare to make sure cyber security is given the time and resources it needs to make the school secure.
- Provide annual training for staff on the basics of cyber security.
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents.
- Put controls in place that will be proportionate, multi-layered, and up to date.
- Regularly review and test its systems.
- Back up critical data regularly.
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our ICT manager.
- Make sure staff dial into our network using a virtual private network (VPN) when working from home.
- Enable multi-factor authentication where possible.
- Store passwords securely using a password manager.
- Have a firewall in place that is switched on.
- Check that its supply chain is secure.

10. Internet access

The school's wireless internet connection will be secure.

10.1 Pupils

The school will provide details of its approach to the use of WiFi by pupils, including any security or filtering settings used.

10.2 Parents/Carers and Visitors

Parents/carers and visitors to the school will not be permitted to use the school's WiFi unless specific authorisation is granted by the headteacher.

11. Monitoring and Evaluation

The headteacher, comp. science lead, in liaison with SchoolCare, will monitor the implementation of this policy, ensuring it is updated to reflect the needs and circumstances of the school. This policy will be reviewed annually.

Updates

Dates	Comments
06.03.25	Updated Social Media section to reflect current presence of school.