ICT ACCEPTABLE USE POLICY

MIDDLEWICH HIGH SCHOOL

Reviewed: November 2025
Date Approved: 10th November 2025
Next Review Date: Autumn Term 2028

The Sir John Brunner Foundation

Document Control Sheet

Document Type	Policy
Document name	ICT Acceptable Use
Originator	Jay Lobina-Lal
Approved by	Full Governing Body
Date approved	10th November 2025
Review interval	Every 3 Years
Date of last approval	November 2025
Date of next review	Autumn Term 2028
Links with other policies	
Equality Act 2010 issues fully considered	Yes – considered to have a neutral impact

Middlewich High School
King Edward Street, Middlewich, Cheshire, CW10 9BU
Tel: 01606 537670

1.Purpose

The purpose of this policy is to:

- ensure that the school complies with all laws and regulations regarding the storage, use, dissemination and transmission of information (see separate 'Legal Basis' document for details);
- ensure that the school's ICT systems are adequately protected against misuse or abuse; and
- ensure that users are aware of, and agree to be bound by, certain responsibilities in their use of the school's ICT systems.

This policy should be read in conjunction with the school's Safeguarding Policy, Behaviour for Learning Policy, and Relationships, Sex and Health Education (RSHE) Policy. This policy supports the school's whole school approach to safeguarding as outlined in Keeping Children Safe in Education (KCSIE) 2025.

2. Scope

The school's ICT systems are provided to staff and students to enable them to better carry out their teaching and learning respectively. For the purposes of this document, 'ICT systems' includes, but is not limited to:

- all hardware devices on the school site, whether owned by the school or not
- all software programs, including all physical media (CD's, disks etc.) on site, whether owned by the school or not, and any electronic implementation thereof;
- all web-based resources including email whether located externally (and accessed from within the school) or internally (and accessed from either within or beyond the school),
- the school's MIS system (Capita SIMS) and
- all network services, wired and wireless.
- generative artificial intelligence (AI) tools and platforms accessed through school systems or for school purposes; - any personal devices used to access school systems or for school-related activities (Bring Your Own Device - BYOD); - cloud-based services and applications used for educational purposes.

3. Acceptable Use Contract

The school requires all authorised users of the school's ICT systems to consent to be bound by this policy. Unauthorised use of the systems or use that is contrary to this policy will result in the relevant disciplinary procedure being followed. This could result ultimately in exclusion of students or dismissal of staff. In the event of a serious infringement the school may also decide to institute legal proceedings under the relevant civil or criminal law (see separate 'Legal Basis' document for details).

Further information relating to acceptable use is available in the school's Online Safety, Data Protection, Child Protection and Safeguarding, Behaviour, and RSHE Policies. All staff must

receive appropriate safeguarding and child protection training (including online safety) at induction, with updates provided at least annually in line with KCSIE 2025. This includes understanding the expectations, applicable roles and responsibilities in relation to filtering and monitoring.

3.1 Safeguarding and Reporting Concerns

All users should be aware that:

- The school's safeguarding policies and procedures are transparent, clear, and easy to understand. Systems are in place that are well promoted, easily understood and easily accessible for children to confidently report any form of abuse or neglect, knowing their concerns will be treated seriously.

- If any user has concerns about a child's welfare related to online activity, they should follow the processes set out in the school's Child Protection and Safeguarding Policy and speak to the Designated Safeguarding Lead (DSL) or a deputy immediately.

- Staff should never promise a child that they will not tell anyone about a report of any form of abuse, as this may ultimately not be in the best interests of the child.

- The school takes a whole school approach to online safety, ensuring that safeguarding and child protection are at the forefront and underpin all relevant aspects of process and policy development.

4. Responsibilities of Users

Physical Devices

Users must take appropriate care of the physical devices owned by the school and loaned to or used by them. The school will review the access granted to such devices in the event that such appropriate care is not taken.

Security

Authorised ICT system users are allocated usernames and passwords to control access to systems. Users' responsibilities in respect of such security are as follows.

- the user is responsible for the confidentiality of the username and password and must take steps to change their password if they believe it has become known to others.
- users must respect any password policies in place from time to time and communicated via Novus.
- users must not use anyone else's username/password without that user's permission.
- users must not obtain or try to obtain anyone else's password without their permission.
- users must inform the IT Technician immediately if they suspect someone else of using another person's username/password.
- teachers must not leave computers unattended when logged in unless they have 'locked' the computer in such a way that their password is required for access.

Generative Artificial Intelligence (AI)

Users must be aware of the following expectations regarding the use of generative AI tools (such as ChatGPT, Google Gemini, Claude, or similar platforms):

- Students may only use generative AI tools when explicitly permitted by their teacher and for specified educational purposes.
- All use of generative AI must be transparent
- students must clearly indicate when AI has been used to support their work.
- Using AI to complete assessed work without permission constitutes academic dishonesty (see Section 7).
- Staff should be aware that filtering and monitoring requirements apply to the use of generative AI in education, in line with DfE guidance 'Generative AI: product safety expectations'.
- Users must not input personal or sensitive information about themselves or others into generative AI tools.
- Users must critically evaluate any information or content generated by AI tools and verify its accuracy.

5. Computer Network and Networked Resources

Users must not connect any device to the network, or to a computer connected to the network, without the permission of Novus.

With the exception of the Senior Leadership Team and Novus, users must not gain access or attempt to gain access to any files owned by someone else unless the owner has specifically granted such access. This does not apply to teachers gaining access to student areas in the course of their academic duties or accessing lessons and units of work for cover or created for the department.

Users must not knowingly introduce malicious code including viruses, network worms, Trojan horses, logic bombs etc and must be mindful at all times of the risk of introducing such code through removable media (such as ‘pen’ drives or memory sticks) and through email attachments.

Users must not install software on school equipment without permission from the IT Technician or Assistant Principal responsible for ICT infrastructure.

Users are entirely responsible for the contents of their email, ‘home directory’, e-portfolio or other area designated for their sole use. The school may delete these areas in their entirety following the cessation of employment or enrolment as a student.

6. Unacceptable use of technology
The following activities are considered unacceptable use of the school's ICT systems:

- Verbal, written or electronically transmitted abuse of any person including indecent or obscene expressions, conduct, or threat of physical abuse to any person.
- Verbal, written or electronically transmitted harassment: defined as behaviour directed at a member of the school community which would cause emotional distress, intimidation,

or coercion to a reasonable person in the victim's position. This includes cyberbullying, prejudice-based and discriminatory bullying.
- Failure to respect the privacy of other individuals through the use of technology, including the unauthorised sharing of images, videos, or personal information. –
- Creating, sharing, or possessing indecent images of children (under 18). Users must be aware that even viewing an indecent image on a computer means that a digital image has been made, which is an offence under the Sexual Offences Act 2003.
- Sharing or distributing images or videos of others without their explicit consent, including 'sexting' or sharing intimate images.
- Use by staff for personal reasons is acceptable except where the activity might reasonably be considered to be contrary to the ethos of the school or bring the school into disrepute.
- Failure by a student to follow the instructions of their teacher or other responsible adult within the school concerning their use of ICT, particularly in respect of the information which they are allowed to access, the applications they are allowed to use, and the resources they are allowed to consume. - Installation of any unauthorised software or applications.
- Storage of non-business related software or documents.
- Any tampering with hardware (e.g. setting a BIOS password, removing casing etc).
- Leaving PCs unattended and logged in for extended periods.
- Use of unapproved screensavers and backdrops.
- Hacking or snooping (e.g. attempting to gain access to areas/systems known to be unauthorised).
- Unauthorised connection of equipment to any part of the school network - in particular laptop computers and personal devices.
- Accessing, creating, storing, or distributing material that contains defamatory, obscene, pornographic, discriminatory, or illegal content.
- Using technology to 'groom' or inappropriately communicate with children or young people.
- Any activity that violates the Equality Act 2010, including material which bullies, harasses, discriminates or encourages discrimination on the grounds of age, disability, gender reassignment, race (including colour, nationality, ethnic or national origins), religion or belief, sex, or sexual orientation.
- Using generative AI or other tools to complete work dishonestly or without appropriate attribution (see Section 7).
- Attempting to bypass or disable filtering and monitoring systems

7 Academic Dishonesty/Cheating

Users must not use ICT systems to cheat in academic assessments. The relevant forms of cheating include the following.

- unauthorised assistance: communication to another through electronic means.
- the unauthorised possession or use of examination or course related material.
- plagiarism: whereby another's work is deliberately used or appropriated without any indication of the source, thereby attempting to convey the impression that such work is the student's own.
- any person who knowingly helps someone else to cheat.

- Using generative AI tools to complete assessed work without explicit permission from the teacher and without appropriate acknowledgement.
- Submitting work generated by AI as one's own original work.
- Using AI to paraphrase or rewrite content without understanding or critically engaging with the material.

8. Responsibilities of System Administrators

The IT Technician and other users with 'systems administration' rights have the same responsibilities as other users, plus additional responsibilities and privileges due to their administrative position. An external IT support provider is retained to proactively monitor the ICT systems and support the IT Technician to maintain them.

Someone with these rights:

- is responsible for establishing appropriate user privileges and monitoring access for the systems they administer;
- is expected to take reasonable precautions to safeguard against corruption, compromise or destruction of data, computer systems, and network resources;
- is expected to maintain the ICT systems in a way that minimises the chance of unauthorised access;
- is expected to ensure that systems security patches, upgrades and software (such as spam filters and anti-virus software) are kept up to date where possible and such that the service is not adversely affected;
- must ensure within reason that all software in use is properly licensed; and
- must ensure adequate backup and disaster recovery procedures are in place, monitored and tested for effectiveness.

System administrators must also ensure that:

- Appropriate filtering and monitoring systems are in place and regularly reviewed to keep children safe online, including in relation to generative AI tools.
- An annual review of the school's approach to online safety is carried out, supported by an annual risk assessment that considers and reflects the risks children face.
- The school's filtering and monitoring systems meet the standards set out in KCSIE 2025 and DfE guidance.
- Records are kept of filtering and monitoring reviews and any incidents or concerns identified.

9. Confidentiality, Privacy and Internet Safety

- Users have a duty of care to protect the confidentiality of any information that they might access through the school ICT systems in the course of legitimate employment activities or through academic studies, in line with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

- The school complies with data protection law as set out in the DfE's 'Data Protection: a toolkit for schools' and ICO guidance 'For Organisations'. Staff, governors and trustees understand how to comply with data protection law, develop appropriate data policies

and processes, know what staff and pupil data to keep, and follow good practices for preventing personal data breaches.

- The school reserves the right to monitor, inspect, copy, review and store at any time and without prior notice any and all usage of the computer network and Internet access and any and all information transmitted or received in connection with such usage. This includes monitoring of generative AI tool usage. All such information files shall be and remain the property of the school and no user shall have any expectation of privacy regarding such materials.

- Monitoring is carried out to:
- Keep children safe online
- Identify safeguarding concerns
- Ensure compliance with this policy and other school policies
- Protect the school's ICT systems from misuse
- Comply with legal obligations

- Always be mindful that people you 'meet' on the Internet may not be who they say they are: never reveal personal details such as addresses, student names, telephone numbers, or photographs to unknown individuals.

- Users should be aware that children may not feel ready or know how to tell someone that they are being abused, exploited, or neglected online, and/or they may not recognise their experiences as harmful. Staff should maintain professional curiosity and speak to the Designated Safeguarding Lead if they have any concerns about a child.

- Staff should be able to reassure victims that they are being taken seriously and that they will be supported and kept safe. A victim should never be given the impression that they are creating a problem by reporting any form of abuse and/or neglect. Nor should a victim ever be made to feel ashamed for making a report.

Acceptable Use and Online Policies – Legal Basis

10. Keeping Children Safe in Education (KCSIE) 2025

This policy is written in accordance with KCSIE 2025, which is statutory guidance that schools must have regard to. KCSIE sets out what schools and colleges must do to safeguard and promote the welfare of children.

Key requirements relevant to this policy include:

- All staff should be aware of systems within the school which support safeguarding, including this acceptable use policy, the child protection policy (which includes procedures to deal with child-on-child abuse), the behaviour policy (which includes

measures to prevent bullying, including cyberbullying, prejudice-based and discriminatory bullying), and the staff behaviour policy (code of conduct).

- All staff should receive appropriate safeguarding and child protection training (including online safety) at induction. The training should be regularly updated. In addition, all staff should receive safeguarding and child protection (including online safety) updates (for example, via email, e-bulletins, and staff meetings), as required, and at least annually.

- The school has appropriate policies and procedures in place, including for online safety, which are transparent, clear, and easy to understand for staff, pupils, parents, and carers.

- The school facilitates a whole school approach to safeguarding, ensuring that safeguarding and child protection are at the forefront and underpin all relevant aspects of process and policy development.

- Where there is a safeguarding concern, the child's wishes and feelings are taken into account when determining what action to take and what services to provide.

11. Relationships, Sex and Health Education (RSHE) Statutory Guidance 2026

This policy supports the delivery of RSHE as set out in the statutory guidance which came into force in September 2026. The acceptable use policy contributes to:

- Teaching pupils about healthy relationships, including online relationships
- Educating pupils about online safety, including the risks of sharing images and information online
- Supporting pupils to understand consent, including in digital contexts
- Helping pupils develop skills to navigate online spaces safely and respectfully
- Teaching pupils about the potential harms of sexual violence and sexual harassment, including online

The school's RSHE curriculum includes age-appropriate teaching about online safety and is delivered as part of a whole school approach to wellbeing and positive relationships.

12. Laws Covering Hacking, Privacy and Protection of Personal Data

12.1 . Computer Misuse Act (1990)

This Act creates three criminal offences.

Unauthorised access to computer material
This makes it illegal to access a computing system unless authorised to do so. As such it makes the activity of "hacking" a crime. It does not matter whether the hacker is remote, working from a distance over the remote area networks, or local, where persons such as employees or students who may have limited authorisation to use the computers but they knowingly exceed that authority. The hacking need not be directed at a particular computer, program or data. For example, it is unlawful, without proper authority:

- to use another person's ID and password in order to access a computer, use data or run a program;
- to alter, delete, copy, or move a program or data, or simply to output a program or data; or
- to lay a trap to obtain a password.

Unauthorised access to a computer system with intent to commit or facilitate the commission of a further offence

This covers the situation where unauthorised access is gained with intent to commit a further offence. For example, a person may gain unauthorised access to a computer via another person's ID in order to transmit offensive material or access confidential material.

Unauthorised modification of computer material

This offence includes the deliberate deletion or corruption of programs or data. It also includes the introduction of viruses etc, where these result in the modification or destruction of data.
The first of these three offences would most likely be dealt with in a magistrates' court, but the other two are considered to be serious and would be referred to the Crown court where very large fines and/or jail sentences are possible.

The Computer Misuse Act also applies to unauthorised access to generative AI systems or attempts to manipulate such systems in ways that exceed authorised use.

13. General data Protection Regulations (2018)

The Data Protection Act 2018 and UK GDPR require that all data relating to living persons should not be stored or processed on a computer system or in a relevant manual file by any person unless the purpose for which that data is stored is registered and lawful. Personal data includes that contained in photographs, videos and CCTV film which would enable a person to be identified.

Central to the legislation are the six Principles which require personal data to be:
- Processed lawfully, fairly and in a transparent manner
- Collected for specified, explicit and legitimate purposes
- Adequate, relevant and limited to what is necessary
- Accurate and, where necessary, kept up to date
- Kept for no longer than is necessary
- Processed in a manner that ensures appropriate security

The principles also provide for individuals to obtain details of the data held about themselves and, where appropriate, to have data corrected or deleted.

The school will not publish images if such permission has been explicitly refused by parents/carers.

Central to the Act are the six Principles which require personal data to be fairly processed, processed only for such purposes for which it is registered, is kept to a minimum for that purpose, kept accurate and up to date and only for such time as is necessary to achieve that purpose and is kept securely. The principles also provide for individuals to obtain details of the data held about themselves and, where appropriate, to have data corrected or deleted.

The school will not publish images if such permission has been explicitly refused by parents/carers.

Staff, governors and trustees should refer to:
- ICO guidance 'For Organisations' which includes information about obligations and how to comply, including protecting personal information and providing access to official information
- DfE 'Data Protection: a toolkit for schools' which helps school staff, governors and trustees understand how to comply with data protection law, develop data policies and processes, know what staff and pupil data to keep and follow good practices for preventing personal data breaches

Users must be particularly careful when:
- Using generative AI tools
- never input personal or sensitive data about pupils, staff or families into AI systems
- Sharing information via email or cloud services - ensure appropriate security measures are in place
- Taking or storing photographs or videos of pupils - ensure appropriate consent has been obtained and images are stored securely

14. Copyright, Designs and Patents Act (1988)
Under this Act it is unlawful to take an unauthorised copy of someone else's work. A person holds the copyright in that work if it is the product of their intellectual activity and hence is their intellectual property, although if that work is done as part of your employment the intellectual property and hence the copyright, is owned by the school. Do not use someone else's work unless:-
- you have that person's permission; or
- you are sure that the material is in the Public Domain; or
- you are sure that the material is not protected by copyright.

Usage includes storing and displaying material electronically.

This Act also applies to content generated by AI tools. While AI-generated content may have complex copyright implications, users should:
- Always attribute when AI tools have been used
- Not claim AI-generated content as their own original work
- Be aware that AI tools may generate content based on copyrighted material
- Seek guidance from staff when unsure about the copyright status of AI-generated material

15. Laws Covering Offences of a Sexual Nature

The Internet is becoming more accessible to minors through computers in homes and schools. Material must not be published which might lead to injury or damage to minors. This includes material which is pornographic or excessively violent. You should be aware that some legitimate research documents may include material of a medical nature which is unsuitable for minors who must, therefore, be protected from unauthorised viewing.

The retention or display of pornographic or sexually-explicit material is forbidden by the school, as is the enablement of links to sites containing such material. This is irrespective of whether that material is legal in this country or any other. The Criminal Justice and Public Order Act 1994 broadens the scope of the Obscene Publications Act 1959 making the storage and electronic transmission of pornographic material arrestable offences.

16. Sexual Offences Act 2003

Grooming

If you are over 18 and have communicated with a child under 16 at least twice (including by phone or internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence.

This includes communication through social media, messaging apps, online gaming platforms, and any other digital means. Staff must maintain professional boundaries at all times and follow the school's staff behaviour policy (code of conduct) regarding communications with pupils.

Making indecent images

It is an offence to take, make, distribute, show, advertise indecent images of a child under 18. (NB even to view an indecent image on your computer means that you have made a digital image.)

This includes:

- 'Sexting' or youth produced sexual imagery
- the creation and sharing of sexual images by young people under 18
- Possessing, distributing or publishing sexual images of anyone under 18, even if the young person has consented
- Viewing such images online, as this constitutes 'making' an image
- Staff must report any incidents involving indecent images of children to the Designated Safeguarding Lead immediately

Causing a child under 16 to watch a Sexual Act

To intentionally cause a child to watch someone else taking part in sexual activity, including looking at images such as videos, photos or webcams, for your own gratification.

Abuse of positions of trust

Staff need to be aware that it is an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Applies to teachers, social workers, health professionals, Connexions PA's etc.)

17. Laws Covering Discrimination and Cyberbullying

Any material which bullies, harasses, discriminates or encourages discrimination on the grounds of age, disability, gender reassignment, race (including colour, nationality, ethnic or national origins), religion or belief, sex orientation or otherwise is in contravention of the Equality Act 2010.

The Equality Act 2010 protects people from discrimination on the basis of protected characteristics. In the context of ICT use, this means:

- Users must not create, share or distribute material that discriminates against or harasses individuals based on protected characteristics
- Cyberbullying on the basis of protected characteristics is taken extremely seriously and will be dealt with in accordance with the school's behaviour policy
- The school has a duty to eliminate discrimination, advance equality of opportunity, and foster good relations
- All users should be aware that 'banter' or 'jokes' that target protected characteristics constitute discrimination and are unacceptable

Online bullying can take many forms including:
- Sending threatening or abusive messages
- Creating fake profiles to humiliate someone
- Sharing embarrassing images or information
- Excluding someone from online groups or activities - Spreading rumours or gossip online

All forms of bullying, including cyberbullying, are addressed in the school's behaviour policy.

Libel
Facts which concern individuals or organisations must be accurate and verifiable. Views or opinions must not portray their subjects in any way which would damage their reputation.

Public Order Act (1986)
It is an offence to possess, publish, disseminate material intended to/likely to incite racial hatred.

This includes material shared online through social media, messaging apps, or any other digital platform. Users must not share or create content that incites hatred or violence against any group.

Telecommunications Act (1984)
It is an offence to send by public telecommunications network any offensive, indecent, obscene or menacing messages that cause annoyance / inconvenience / needless anxiety.

This applies to all forms of electronic communication including email, text messages, social media messages, and communications through apps and platforms.

Malicious Communications Act (1988)

It is an offence to send a letter or article which includes indecent, grossly offensive, threatening or false information with the intent of causing anxiety/stress to the recipient.

This Act applies to electronic communications as well as physical letters. Users must not send messages or content intended to cause distress to others.

Protection from Harassment Act (1997)
Section 1 - A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.
Section 4 - A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Online harassment, including persistent unwanted contact, threatening messages, or campaigns of abuse through digital means, is covered by this Act. A 'course of conduct' means behaviour on at least two occasions and can include online behaviour.

18. Incitement
Users must not publish anything which might incite others to commit criminal acts or even to contemplate them.

19. Communications Act 2003

Section 127 of the Communications Act 2003 makes it an offence to send a message or other matter via a public electronic communications network that is:
- Grossly offensive, indecent, obscene or menacing in character; or
- Sent for the purpose of causing annoyance, inconvenience or needless anxiety

This applies to messages sent via:
- Email
- Social media platforms
- Messaging apps
- Online forums or comment sections
- Any other electronic communications network

Users should be aware that offensive or threatening online communications can result in criminal prosecution.

20. Online Safety Act 2023
The Online Safety Act 2023 places duties on online service providers to protect users, particularly children, from harmful content. While this Act primarily regulates service providers rather than users, schools and users should be aware that:
- Online platforms have duties to remove illegal content and protect children from harmful content
- Users can report harmful content to platforms and expect it to be addressed
- The Act strengthens protections against online abuse, particularly for children
- Schools should teach pupils about how to report harmful content and stay safe online

The school's online safety education programme includes teaching pupils about:

- How to recognise harmful or inappropriate content
- How to report concerns to trusted adults and to platforms
- How to protect themselves online
- Their rights and responsibilities as digital citizens