ICT Acceptable use Policy

Secondary Schools

Reviewed:	**Finance Committee**
Approved:	**March 2026**
Next Review:	**March 2029**

Contents

1. Introduction and Acceptance

a) Policy Purpose and Summary

Information and communications technology (ICT) is an integral part of the way our school works, and is a critical resource for pupils, staff (including senior leadership teams), governors, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the school.

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

The policy should be read in conjunction with the WNAT online safety policy. Copies are found on the school website and school intranet.

This policy aims to:

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

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

b) Acceptance

Each member of Staff or Student will be Issued with a Windows Account. The policy will be displayed by default during logon and the user has to accept the policy before the logon process continues. The acceptance is logged electronically. Any amendments to the policy will force the process of acceptance again.

2. Definitions

- **"ICT facilities":** includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service.
- **"Users":** anyone authorised by the school to use the ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.
- **"Personal use":** any use or activity not directly related to the user's study or purpose.
- **"Authorised personnel":** employees authorised by the school to perform systems administration and/or monitoring of the ICT facilities.
- **"Materials":** files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites and blogs.

3. Password Security

3.1 Secure and strong passwords are essential to protect the integrity of ICT systems. Passwords should be long, for example, you could use a long lyric or a memorable phrase plus a number. Do not choose a password which is so complex that it is difficult to remember without writing it down. Your password must not be disclosed to anyone else.

3.2 Your password should be difficult to guess, for example, you could base your password on something memorable that no-one else would know. You should not use information which other people might know, or be able to find out, such as your address or your birthday.

3.3 You must not use a password which is used for another account. For example, you must not use your password for your private email address or online services for any Academy account.

3.4 Passwords (and any other security credential you are issued with such as a key fob or USB drive) must be kept secure and confidential and must not be shared with, or given to, anyone else. Passwords should not be written down.

3.5 You must only use your own login and password when logging into ICT systems. Passwords must be changed whenever there is a system prompt to do so or where there is a possibility that there could otherwise be a possible compromise of the system. Passwords should not be re-used or recycled across different systems.

3.6 Where temporary passwords are issued to any individual, for any reason, then they should be changed at first logon to a permanent password.

3.7 Failure to comply with these requirements could lead to you compromising the school's system security and would be considered a breach of this policy.

4. Unacceptable Use

The following is considered unacceptable use of the school's ICT facilities by any member of the school community. Any breach of this policy may result in disciplinary or behaviour proceedings).

Unacceptable use of the school's ICT facilities includes:

- Using the school's ICT facilities to breach intellectual property rights or copyright
- Using the school's ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- 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 (also known as sexting or youth-produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, its pupils, or other members of the school community

- Connecting any device to the school's ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the school's network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the school
- Using websites or mechanisms to bypass the school's filtering mechanisms
- Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way

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

5. Acceptable Use of E-mail

- All students have been provided with a school email. This email address allows communication within the school community, along with access to specific online software relevant to the study of the school curriculum.
- The Schools systems are suitably protected and are the secure and authorised means of conducting work related correspondence.
- All communications made via school email accounts must be of a tone and nature that respects others.
- Email cannot be regarded as purely private, only to be seen by the receiver.
- All online activity, both in the school and outside, using the school email account must not bring the school into disrepute.
- Communications via the school email accounts may be monitored from time to time.
- Authorised ICT staff may access your school email account if there are concerns about the content of emails, particularly from a safeguarding point of view or if required to do so by law enforcement authorities.
- It is forbidden, at all times, to send files through internal or external email that contain discriminatory, abusive, pornographic, obscene, illegal, offensive, potentially libellous, or defamatory content.

6. Pupil Access to ICT Facilities

6.1 All pupils have access to all student computers in the school, providing they are under the supervision of staff. Some students may have access to loan equipment from the school. Loan equipment should be treated in exactly the same way as ICT equipment based in the school, and as such, use of this equipment is covered by this policy. All loan equipment is for the express purpose of supporting the student's education.

6.2 Students in the 6th form may use school computers outside of the normal school day providing staff from the 6th form team are aware. Sixth form students must not continue to use these facilities after 5pm unless supervised by staff.

6.3 Sixth form students may also have access to the school WIFI system. The WIFI system is secured and students should speak with the networking department or 6th form team for access approval. Use of school WIFI is limited to school work and research and should not be used to download or stream video or music.

6.4 Students are not allowed to:

- Access any computer that would normally be used by the teacher (these would normally be on the teachers' desk)
- Access to computers in IT suites unless under the supervision of staff

6.5 Students are not permitted to install software on any computer or network system, nor modify the equipment in any way.

6.6 Students may use their printing budget to print from the school computers. Any printing must be related to the work of the student. Use of resources to print material not related to school or the work of the student may result in the student/Parents/Carers being invoiced for the printing.

6.7 Google Drive should be used to store work that needs to be taken home. The use of USB drives is not permitted unless written authorisation has been obtained.

7. Unacceptable Use of ICT and the Internet Outside of School

The school will sanction pupils, in line with the school's behaviour policy if a pupil engages in any of the following at any time (even if they are not on school premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the school's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams (also known as sexting or youth produced sexual imagery)
- Activity which defames or disparages the school, or risks bringing the school into disrepute
- Sharing confidential information about the school, other pupils, or other members of the school community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the school's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Wilful or intentional damage to ICT facilities or materials will result in the parent(s) being invoiced for the full cost of replacement of the facilities or materials.

The school reserves the right to withdraw student access to ICT facilities in the school for considerable or persistent infringements of the policy, or engagement in any of the above activities. The school may also contact the Police where appropriate.

8. Viruses

8.1 Viruses can expose the trust to very considerable risks.

8.2 You are required to take all reasonable steps to avoid the introduction of any virus on the school equipment, systems or networks.

8.3 Reasonable steps will include, but are not limited to:

- ensuring that files downloaded from the internet, received via email or on removable media such as a memory stick are checked for any viruses using the school anti-virus software before being used;
- be cautious when opening any emails that you are not expecting especially those that contain an attachment;
- do not follow any links to questionnaires, offers, requests, etc. from unknown sources – delete the email;
- do not forward any suspect emails to anybody: Delete it;
- delete emails with attachments that you were not expecting even if you know the person sending, if the wording seems “odd” in some way. These programs can often spoof the Sender field in emails to make it look like someone you know is emailing you;
- not installing any hardware or software
- allowing any anti-virus software installed on school ICT equipment to run as it needs to and not interrupting or in any way interfering with such software;
- ensuring that any ICT equipment provided by the school for use off site, benefits from regular school anti-virus updates either by providing it to the ICT staff so that such updates can be undertaken.

8.4 If you suspect there may be a virus on any ICT equipment, you must stop using the equipment and speak to a teacher or a member of the Networking team immediately.

8.5 Report any attempted phishing e-mail to your teacher in order that they can make sure that investigations can be made into potential other users receiving the email. Often a phishing e-mail is sent to a number of people.

9. Artificial Intelligence (AI or Generative AI)

9.1 Students are expected to use AI tools responsibly and avoid plagiarism in their academic work.

9.2 Not use AI applications to gain unfair advantages in group assignments or assessments.

9.3 Where AI generated content is used in work it must be clearly referenced, including the name of the AI tool, date the content was generated, explanation of how you used it and a screenshot of the questions asked and answers received.

9.4 Students must use AI technologies in a manner that respects the rights and well-being of their peers, teachers, and staff.

9.5 Avoid using AI applications to generate or share content that may be offensive, discriminatory, or harmful.

10. School ICT Equipment at Home

10.1 Students may be supplied with equipment to utilise at home including desktop computers, laptops and WIFI dongles

10.2 Such equipment must be treated and used in the same way as it would be in the workplace. You are expected to abide by this policy when using all such equipment. This means that you remain liable for the use of the equipment and the passwords for it.

10.3 On request you must make portable and mobile ICT equipment available for anti-virus updates and software installations, patches or upgrades. The installation of any applications or software packages is not permitted. You must not make copies of any school software for use outside the organisation or outside the rules prescribed by the particular software's license.

10.4 You are responsible for ensuring that all equipment is stored and kept safely and securely. Any protective equipment must be utilised properly.

10.6 If or when you leave the school, you must return all ICT equipment to the school

10.7 The School reserves the right to inspect all equipment utilised at home. The school retains the right to verify equipment for audit purposes at any time throughout the duration of its use. Students and Parents/Carers are therefore obliged to produce any equipment within a reasonable timeframe (5 working days) where requested to assist with this verification process.

11. Incident Reporting

11.1 Concerns regarding virus, phishing emails, unsolicited emails, any unauthorised use or suspected misuse of ICT or any of matter of concern, should be reported to your manager and to relevant ICT staff, as a matter of urgency.

11.2 In the event that you receive an email, through your professional email account, either from within the school community or from any third party that you consider to be abusive then that should immediately be reported a teacher or by emailing bullying@wnat.co.uk .

12. Sanctions for Unacceptable Use

- Parents/Carers will be informed as soon as possible.
- A temporary or permanent ban from Internet access.
- A temporary or permanent ban from the use of school's ICT facilities.
- Access to the Internet may be withdrawn.
- A serious breach of the policy will result in further disciplinary action being taken, including exclusion.
- If it is suspected that a criminal offence has been committed the appropriate authorities will be informed.
- Appropriate additional disciplinary action if the action breaks any other school rule or convention.
- Where applicable, referral to appropriate external agencies.

13. Search and Deletion

Under the Education Act 2011, and in line with the Department for Education's guidance on searching, screening and confiscation, the school has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under school rules or legislation.

The school can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break the school's rules.

Staff members may also confiscate devices for evidence to hand to the police, if a pupil discloses that they are being abused and that this abuse contains an online element.

14. Parents/Carers

14.1 Access to ICT Facilities and Materials

Parents/Carers do 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 (for instance, as a volunteer or as a member of the PTA) may be granted an appropriate level of
access, or be permitted to use the school's facilities at the headteacher's discretion.

The school may also make available access to the school system for Parents/Carers who do not have internet access, to allow them to attend virtual Parents/Carers' evenings. If a parent needs to access school ICT facilities for this they should, in the first instance, contact the relevant year office.

Where Parents/Carers are granted access in this way, they must abide by this policy as it applies to staff.

14.2 Communicating With or About the School Online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents/Carers 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.

15. Relevant Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018
- The General Data Protection Regulation
- Computer Misuse Act 1990
- Human Rights Act 1998
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- The Education and Inspections Act 2006
- Keeping Children Safe in Education 2021
- Searching, screening and confiscation: advice for schools
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Appendix 1: Parent/Carers Acceptable Use Policy

1. I have read and discussed the School Acceptable Use Policy with my child.
2. I know that my child will receive online safety education to help them understand the importance of safe use of technology and the internet, both in and out of school.
3. I am aware that any internet and computer use using school equipment may be monitored for safety and security reasons, to safeguard both my child and the schools' systems. This monitoring will take place in accordance with data protection (including GDPR) and human rights legislation.
4. I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
5. I understand that if the school has any concerns about my child's safety online, either at school or at home, then I will be contacted.
6. I understand that if my child does not abide by the school Acceptable Use Policy then sanctions will be applied in line with the school policies including behaviour, online safety and anti-bullying policy. If the school believes that my child has committed a criminal offence, then the Police will be contacted.
7. I, together with my child, will support the school's approach to online safety and will not deliberately upload or add any images, video, sounds or text that could upset, threaten the safety of or offend any member of the school community. I will not share other pupils work on social media.
8. I know that I can speak to the school Designated Safeguarding Lead, my child's pastoral manager or the headteacher if I have any concerns about online safety.
9. I will visit the school website for more information about the school's approach to online safety as well as to access useful links to support both myself and my child in keeping safe online at home.
10. I will visit the following websites for more information about keeping my child(ren) safe online:
    - www.thinkuknow.co.uk/Parents/Carers,
    - www.nspcc.org.uk/onlinesafety
    - www.internetmatters.org
    - www.saferinternet.org.uk
    - www.childnet.com
11. I will support the school and my child by role modelling safe and positive online behaviour (such as sharing images, text and video responsibly) and by discussing online safety with them when they access technology at home.

West Norfolk Academies Trust
Acceptable Use Policy – Parent/Carer Response

I have read, understood and agree to comply with the School Acceptable Use Policy (AUP).

Pupil name……Form…… Date…….

School ……...

Parents/Carers

Parents/Carers Signature……. Date……...