West Norfolk Academies Trust

SHS

Springwood

High School

ICT ACCEPTABLE USE POLICY

Students & Parents

Reviewed by: Governing Body

Approved: February 2022

Next review date: February 2026

Contents

1. Introduction

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 online safety policy and WNAT ICT Acceptable Use policy.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for pupils and parents
- 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 user pupil and parent users of our school's ICT facilities.

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

2. 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

3. 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 users' 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

4. Password Security

4.1 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.

4.2 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.

4.3 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.

4.4 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.

4.5 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.

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

4.7 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.

5. 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.

6. 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.
- Springwood's 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 Springwood, 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.

7. Pupil Access to ICT facilities

7.1 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.

7.2 Students in the 6th form have access to the computers in the Hub, O11 and 6th form study area. Students may use these 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.

7.3 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. Use of school WIFI is limited to school work and research and should not be used to download or stream video or music.

7.4 Students are not allowed access to:

- Any computer that would normally be used by the teacher (these would normally be on the teachers' desk)
- Access to computers in Mu1, Mu2, Mu3, Mu4, JL1, T3 or T4 unless under the supervision of staff

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

7.6 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 being invoiced for the printing.

7.7 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.

8. 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.

9 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.

10. Parents

10.1 Access to ICT facilities and materials

Parents do not have access to the school's ICT facilities as a matter of course.

However, parents 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 who do not have internet access, to allow them to attend virtual parents' 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 are granted access in this way, they must abide by this policy as it applies to staff.

10.2 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 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.

11. Viruses

11.1. Viruses can expose Springwood High School to very considerable risks.

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

11.3. 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.

11.4. 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.

11.5. 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.

12. Springwood High School ICT equipment at home

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

12.2. 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.

12.3. 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.

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

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

12.7. Springwood High 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 are therefore obliged to produce any equipment within a reasonable timeframe (5 working days) where requested to assist with this verification process.

13. **Incident reporting**

13.1 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.

13.2 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@springwoodhighschool.co.uk .

Appendix 1

Springwood High School

Loan agreement for pupils

1. This agreement is between:

1) Springwood High School.

2) The parent and student.

And governs the use and care of devices assigned to the parent's child (the "pupil"). This agreement covers the period from the date the device is issued through to the return date of the device to Springwood High School.

All issued equipment shall remain the sole property of the Springwood High School and is governed by Springwood High School's policies.

1. Springwood High School is lending the pupil a device ("the equipment") for the purpose of doing educational work from home.

2. This agreement sets the conditions for taking a device ("the equipment") home.

I confirm that I have read the terms and conditions set out in the agreement and my signature at the end of this agreement confirms that I and the pupil will adhere to the terms of loan.

2. Damage/loss

By signing this agreement I agree to take full responsibility for the loan equipment issued to the pupil and I have read or heard this agreement read aloud and understand the conditions of the agreement.

I understand that I and the pupil are responsible for the equipment at all times.

If the equipment is damaged, lost or stolen, I will immediately inform Springwood High School and I acknowledge that I am responsible for the reasonable costs requested by the school to repair or replace the equipment. If the equipment is stolen, I will also immediately inform the police.

I agree to keep the equipment in good condition and to return it to Springwood High School on their demand in the same condition.

I will not leave the equipment unsupervised in unsecured areas.

I will make sure my child takes the following measures to protect the device:

- Keep the device in a secure place when not in use
- Don't leave the device in a car or on show at home
- Don't eat or drink around the device
- Don't lend the device to siblings or friends
- Don't leave the equipment unsupervised in unsecured areas

3. Unacceptable use

I agree that my child will not carry out any activity that constitutes ‘unacceptable use’.

This includes, but is not limited to the following:

- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Activity which defames or disparages Springwood High School, or risks bringing the education provider into disrepute
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language
- Accessing inappropriate or offensive material online

I accept that the pupil will be disciplined via the appropriate channels (Springwood High School and care workers) if they engage in any of the above **at any time.**

4. Personal use

I agree that the pupil will only use this device for educational purposes and not for personal use and will not loan the equipment to any other person.

5. Data protection

I agree to take the following measures to keep the data on the device protected.

- Make sure my child locks the equipment if it’s left inactive for a period of time
- Do not share the equipment among family or friends
- Update antivirus and anti-spyware software as required
- Install the latest updates to operating systems, as prompted

If I need help doing any of the above, I will contact my Springwood High School and seek guidance.

6. Return date

I will return the device in its original condition to A Springwood High School employee within fourteen days of being requested to do so.

7. Consent

By signing this form, I confirm that I have read and agree to the terms and conditions set out above.

PUPIL’S FULL NAME	
PARENT’S FULL NAME	
PARENT’S SIGNATURE	