THE WILLOW TREE FEDERATION
COMMUNITY PRIMARY SCHOOL

ICT and Acceptable Use Policy

Mission Statement
The children are at the heart of everything we do at Willow Tree Federation. We take a holistic approach to child development and we are privileged to support our children, families and the wider community to change and enhance lives. We celebrate the wide diversity of the backgrounds, beliefs, talents and interests of our children and we recognise learning happens in communities and empowers them. As a federation at the heart of its community, we understand and respect the positive impact we can have. We plant the seed that grows the future!

Date written	September 2022
Written by:	Headteacher and staff
Date approved by staff:	January 2023
Date Formally Approved by Governors	January 2023
Date Policy became effective	January 2023
Review Date	Reviewed September 2023- no changes (next review September 2024)
Date added to Website:	January 2023

INTRODUCTION

The AUP – Acceptable Policy – relates to the use of technology and should be read in conjunction with the Staff Handbook/Code of Conduct. 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 federation. However, the ICT resources and facilities our schools use also pose risks to data protection, online safety and safeguarding. It is our duty to ensure that ICT is used safely and responsibly. All staff members and Governors are aware of their individual responsibilities when using technology and must adhere to this AUP at all times. Any concerns or clarification should be discussed with the Headteacher.

All Staff, Governors and visitors:

- understand that ICT includes a wide range of systems, including mobile phones, digital cameras, laptops and tablets.
- understand that it is a disciplinary offence to use the school ICT equipment, including email and cameras, for any purpose not permitted by its owner.
- using school equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- will only use the school's email / internet / intranet etc and any related technologies for uses permitted by the Head or Governing Body.
- will ensure that data is kept secure and is used appropriately as authorised by the Head or Governing Body. No passwords should be divulged.
- understand that their use of the internet may be monitored and if anything untoward is uncovered, could be logged and used in line with any disciplinary procedures. This includes all school owned devices.
- will not install any hardware or software on any school owned device without permission. At The Willow Tree Federation this is done by the Technician from Tech Hub.
- know that personal devices must only be used in the context of school business with the explicit permission of the Head. Personal mobile phones should not be used in the presence of children.
- must not use their own phone for taking any photographs of pupils and/or related to school business without written permission from the headteacher (see Appendix B: this will only be granted to teaching staff employed directly by the school). School iPads and cameras should be used for photographs related to school activities (e.g. trips).
- know images will only be taken, stored and used for purposes within school unless there is parental permission for alternative use. On joining school, our parents are asked to sign if they agree to their children's images being used.
- must only use photos of children in accordance with parents' agreement. At our school parents give permission for photos to be taken and used in wider environment e.g. website, taken and sued internally e.g. displays or not taken at all. It is adults' responsibility to know who can have images taken, used and shared.
- must only use photos in accordance with the school's data protection policy and GPDR.
- know photography by parents at school events, such as sports days and school productions, is allowed with the proviso that no images are shared without the permission of all in the image.
- will make every effort to comply with copyright and intellectual property rights.
- will report any incidents of concern regarding staff use of technology, online safety and/or children's safety to the DSL (Lucy Naylor, Duncan Webster or Kirsty Banks) in line with our school's Safeguarding and CP Policy and Online Safety Policy.

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 headteacher 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.

Exceptions from unacceptable use

Where the use of school ICT facilities (on the school premises and/or remotely) is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the headteacher's discretion.

Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the school's policies on Staff Code of Conduct and Behaviour.

Access to school ICT facilities and materials

The school's IT support (Tech Hub) and School's Digital Support Services manage access to the school's ICT facilities and materials for school staff. That includes, but is not limited to:

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

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the school's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the headteacher/school bursar/Tech Hub.

Use of phones and email

The federation provides each member of staff with an email address.

This email account should be used for work purposes only.

All work-related business should be conducted using the email address the school has provided.

Staff must not share their personal email addresses with parents and pupils, and must not send any work-related materials using their personal email account.

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

Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.

If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive or confidential information, the user must 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 must inform the headteacher immediately and follow our data breach procedure.

Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the school to conduct all work-related business.

School phones must not be used for personal matters.

Personal use

Staff are permitted to occasionally use school ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The headteacher may withdraw permission for it at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during teaching hours
- Does not constitute 'unacceptable use', as defined above
- 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 may 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 (see section 5.5). Where breaches of this policy are found, disciplinary action may be taken.
Staff should be aware that personal use of ICT (even when not using school ICT facilities) can impact on their employment by, for instance, putting personal details in the public domain, where pupils and parents could see them.
Staff should take care to follow the school's guidelines on social media and use of email to protect themselves online and avoid compromising their professional integrity.

Personal social media accounts

Members of staff should ensure their use of social media, either for work or personal purposes, is appropriate at all times.

Remote access

We allow selected staff to access the school's ICT facilities and materials remotely. They should dial in using a virtual private network (VPN).
Staff accessing the school's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the ICT manager (Tech Hub)/headteacher may require from time to time against importing viruses or compromising system security.
Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy.

School social media accounts

The school has an official Facebook page, managed by the headteacher, deputy headteacher, nursery teacher and office staff. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.
The school has guidelines (see Appendix C) for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they abide by these guidelines at all times.

Tapestry

Staff in EYFS and Year1 use Tapestry. This is a secure, online journal, which is used to share children's learning and progress with parents/carers. On joining the school, parents and carers are informed about the use of Tapestry and give consent for its use in school. Only named parents/carers are given access to their child's account. If other children appear in pictures shared on the account they are not named and permission for sharing images must have been granted by parents/carers. All applicable social media and acceptable use guidance contained in this framework must be followed. Only named staff authorised by the headteacher, including the EYFS/Year 1 teacher(s), EYFS HLTA, may post and access Tapestry.

Monitoring of school network and use of ICT facilities

The school reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.
The school monitors 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

Pupil Access to ICT facilities
Computers, tablets and equipment are available to pupils only under the supervision of staff.

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.

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 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

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

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.

Data security
The school is responsible for making sure it has the appropriate level of security protection and procedures in place. It therefore takes steps to protect the security of its computing resources, data and user accounts. However, the school cannot guarantee security. Staff, pupils, parents and others who use the school's ICT facilities should use safe computing practices at all times.

Passwords
All users of the school's ICT facilities should set strong passwords for their accounts and keep these passwords secure.
Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.
Members of staff or pupils who disclose account or password information may face disciplinary action.
Parents or volunteers who disclose account or password information may have their access rights revoked.

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

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the school's ICT facilities.
Any personal devices using the school's network must all be configured in this way.

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

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 are managed by ICT manager (Tech Hub).
Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the headteacher immediately.
Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

Encryption
The school ensures that its devices and systems have an appropriate level of encryption.
School staff may only use personal devices (including computers and USB drives) to access school data, work remotely, or take personal data (such as pupil information) out of school if they have been specifically authorised to do so by the headteacher.
Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

Protection from cyber attacks
The school will:

Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the school secure
Provide 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
Investigate whether our IT software needs updating or replacing to be more secure
Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
Put controls in place that are:
- **'Proportionate'**
- **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
- **Up-to-date:** with a system in place to monitor when the school needs to update its software
- **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be

Make sure staff:
- Dial into our network using a virtual private network (VPN) when working from home
- Enable multi-factor authentication where required (e.g. CPOMS)
- Store passwords securely

Make sure ICT staff conduct regular access reviews to make sure each user in the school has the right level of permissions and admin rights
Have a firewall in place that is switched on

Internet access
The school wireless internet connection is secured. Filters are used to reduce the possibility of accessing inappropriate sites from the school network.

Pupils
Pupils may only access the school wi-fi network on school devices for the purposes of education. Pupils are supervised when using devices connected to the school network and wi-fi.

Parents and visitors
Parents and visitors (see Appendix A) to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher/school bursar. If granted, guests will access the Guest Wi-Fi network.
The headteacher will only grant authorisation if:
- Parents are working with the school in an official capacity (e.g. as a volunteer)
- Visitors need to access the school's Wi-Fi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the Wi-Fi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

Monitoring and review

The headteacher will monitor the implementation of this policy, including ensuring it is updated to reflect the needs and circumstances of the school.
This policy will be reviewed every 3 years.

Related policies

This policy should be read alongside the school's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff code of conduct/handbook
- Data protection

Appendix A

Acceptable use of the school's ICT facilities and the internet: agreement for supply staff, volunteers and visitors to The Willow Tree Federation Primary School

Name of supply staff/volunteer/visitor:

When using the school's ICT facilities and/or accessing the internet in school grounds I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the school's reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the school's network
- Share my password with others or log in to the school's network using someone else's details
- Share confidential information about the school, its pupils or staff, or other members of the community
- Access, modify or share data I'm not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the school

I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
I will take all reasonable steps to ensure that devices are secure and password-protected and keep all data securely stored in accordance with the ICT and AUP policy and the school's data protection policy.
I will let the designated safeguarding lead (DSL) know if a pupil informs me they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.
I will report any accidental access to, or receipt of inappropriate materials, or filtering breach to the DSL who will log the incident and take appropriate action. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Parents and visitors to the school will not be permitted to use the school's Wi-Fi unless specific authorisation is granted by the headteacher/school bursar. If granted, guests will access the Guest Wi-Fi network. The access password must not be shared with others. I will not use my personal mobile telephone in areas used by pupils without explicit permission from the headteacher. Personal devices must never be used for photographs of children. I will always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed (supply staff/volunteer/visitor):	**Date:**

Appendix B

Permission and agreement for using a personal device for photographs in school or on educational/sporting visits

Name of teaching staff:

This agreement is in addition and applies in conjunction with the ICT and AUP, Staff Code of Conduct, Data Protection, Online Safety Safeguarding and Child Protection Policies.

Permission is granted for the following period:
Between _____ and
_____ (dates)

Description of the device for which permission is granted:
Type: camera/phone/tablet/other Make: _____ Model: _____

Permission is granted to use a specified personal device to take photographs of pupils solely for the purposes of school business. When using a personal device to take photographs in school or on educational/sports visits, I agree:

- to only take photographs in public/communal shared areas
- to only take photographs in the presence of other adults employed by the school
- to only take photographs necessary for school business
- to only take photographs at school or on an educational or sporting visit
- there must be a clear rationale and consideration of the purpose for any photographs taken and this purpose must be directly concerned with school business
- all photographs taken must adhere to the policies set out above and the school values
- to accept responsibility for transferring photographs to the school SharePoint, blog or Facebook site as soon as possible
- to delete all photographs taken for school purposes as soon as they have been transferred
- to accept responsibility for ensuring parental permission is given for the inclusion and use of any photographs of any pupils captured in a photograph
- to not make copies or share any photographs of pupils via a personal device
- permission only applies while directly employed by the school
- permission is only granted for the device described below

- permission is only granted between the dates given above (permission is rescinded after the last date)

Signed (staff member):	**Date:**
Signed (headteacher):	**Date:**

Appendix C

Guidance for the use of the school website and school Facebook page

The school has an official Facebook page and website, managed by the headteacher, deputy headteacher, office staff and nursery teacher. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

We post or publish:

- dates or announcements about school events or events linked to the school's business
- letters and information about the school and for parents regarding children's education or school life
- photographs, videos and descriptions of children's learning, experiences and achievements
- information or posts from other schools, charities and other groups that we think will be of interest or benefit to our children's families

Messages and replies

- We welcome any likes, feedback and positive comments from families and friends of the school.
- We may not reply individually to all messages we receive, but we will pass on any helpful or positive comments to relevant classes and colleagues.
- We will only 'like' Facebook pages with a non-commercial interest - being 'liked' by us doesn't imply endorsement of any kind.
- We will not get involved in discussions relating to specific incidents, children or issues. If parents/carers/families have any concerns, sensitive questions, complaints or negative comments to share, they should be directed to contact the headteacher using the contact details on our website and Facebook page.

Staff must not upload or post anything to the school website or Facebook page that:

- is confidential to the school/trust or its staff
- amounts to bullying
- amounts to unlawful discrimination, harassment or victimisation
- brings the school/trust into disrepute
- contains lewd, sexually explicit, threatening or similarly inappropriate or offensive comments, images or video clips
- undermines the reputation of the school and/or individuals
- is defamatory or knowingly false
- breaches copyright
- is in any other way unlawful

We will delete:

- abusive, racist, sexist, homophobic or inflammatory comments
- comments we consider to be spam
- personal information, such as telephone numbers, address details, etc.
- posts that identify individual staff members
- posts that advertise commercial activity or ask for donations