



Alfred Lord Tennyson School	Page 1 of 28
ICT Acceptable Use Policy	Issued: December 22
	Review date: December 24
APPROVAL BY	FULL GOVERNING BODY

ICT Acceptable Use Policy

Table of Contents

1. Introduction and aims.....	2
2. Relevant legislation and guidance	2
3. Definitions.....	3
4. Unacceptable use.....	3
4.1. Exceptions from unacceptable use.....	4
4.2. Sanctions.....	4
5. Staff (including governors, volunteers, and contractors)	4
5.1. Access to school ICT facilities and materials	4
5.1.1. Use of phones and email	4
5.2. Personal use.....	5
5.2.1. Personal social media accounts	6
5.3. Remote access	6
5.4. School social media accounts	6
5.5. Monitoring of school network and use of ICT facilities.....	6
6. Pupils.....	6
6.1. Access to ICT facilities.....	6
6.2. Search and deletion.....	7
6.3. Unacceptable use of ICT and the internet outside of school	7
7. Parents	7
7.1. Access to ICT facilities and materials.....	7
7.2. Communicating with or about the school online.....	8
8. Data Security.....	8
8.1. Passwords	8
8.2. Software updates, firewalls, and anti-virus software	8
8.3. Data protection.....	8
8.4. Access to facilities and materials.....	8
8.5. Encryption.....	9

9.	Internet Access.....	9
9.1.	Pupils.....	9
9.2.	Parents and visitors	9
10.	Monitoring and review	9
11.	References.....	9
12.	Safeguarding.....	10
Appendix 1.	Facebook cheat sheet for staff	12
Appendix 2.	Acceptable use of the internet: agreement for parents and carers	14
Appendix 3.	Acceptable use agreements for pupils	15
Appendix 4.	Acceptable use agreement for staff, governors, volunteers and visitors ..	18
Appendix 5.	Equipment Loan Form for Staff	19
Appendix 6.	Device Loan Agreement for Staff	21
Appendix 7.	Device Loan Agreement for Pupils	24
Appendix 8.	Equipment Loan Form for Pupils	27

1. Introduction and aims

ICT is an integral part of the way our school works, and is a critical resource for pupils, staff, 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.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- 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 users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors and visitors.

2. Relevant legislation and guidance

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

- Data Protection Act (2018) [1]
- General Data Protection Regulation [2]
- Computer Misuse Act 1990 [3]

- Human Rights Act 1998 [4]
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 [5]
- Education Act 2011 [6]
- Freedom of Information Act 2000 [7]
- The Education and Inspection Act 2006 [8]
- Keeping Children Safe in Education 2022 [9]
- Searching, screening and confiscation at school [10]

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’ employment, 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. 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 (see section 4.2 below).

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
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- 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

This is not an exhaustive list. The school reserves the right to amend this list at any time. The Headteacher or School Office Manager 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.

4.1. Exceptions from unacceptable use

Where the use of school ICT facilities 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.

4.2. 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 Disciplinary Policy [11] and Staff Code of Conduct [12].

5. Staff (including governors, volunteers, and contractors)

5.1. Access to school ICT facilities and materials

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

Staff will sign a Device Loan Agreement and Equipment Loan Form upon receipt of school IT equipment (see Appendix 5 and Appendix 6)

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 or School Office Manager.

5.1.1. Use of phones and email

The school 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 [1] 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 which contains the personal information of another person, they must inform the Headteacher or School Office Manager 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.

Staff who are provided with mobile phones when leading out of school visits must abide by the same rules for ICT acceptable use as set out in section 4.

5.2. 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. Personal use is permitted provided that such use:

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

Staff 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 (see section 5.2.1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1. Personal social media accounts

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

The school has guidelines for staff on appropriate security settings for Facebook accounts (see section 5.4).

5.3. Remote access

We allow staff to access the school's ICT facilities and materials remotely.

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. 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 [13].

5.4. School social media accounts

The school has an official Facebook page. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

5.5. 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
- 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

6. Pupils

6.1. Access to ICT facilities

Computers and equipment in the school's ICT suite are available to pupils only under the supervision of staff.

Pupils will be provided with accounts linked to the school's virtual learning platforms; these include:

- Purple Mash
- PiXL Times tables
- PiXL Spelling
- Math/Spelling Shed

Parents of pupils who are given devices to loan during bubble closures, or local lockdowns, will sign a Device Loan Agreement and Equipment Loan Form upon receipt of school IT equipment (see Appendix 7 and Appendix 8).

6.2. Search and deletion

Under the Education Act 2011 [6], and in line with the Department for Education's guidance on Searching, screening and confiscation [10], 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.

6.3. Unacceptable use of ICT and the internet outside of school

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

- Using ICT or the internet to 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
- 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

7. Parents

7.1. 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.

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

7.2. *Communicating with or about the school online*

We 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.

We ask parents to sign the agreement in Appendix 2.

8. Data Security

The school 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.

8.1. *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.

8.2. *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.

8.3. *Data protection*

All personal data must be processed and stored in line with data protection regulations and the school's Data Protection Policy [13].

8.4. *Access to facilities and materials*

All users of the school's ICT facilities will have clearly defined access rights to school systems, files and devices.

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 School Office Manager 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.

8.5. 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.

9. Internet Access

The school wireless internet connection is secured.

9.1. Pupils

Pupil are only permitted to use the internet when supervised by an adult.

9.2. Parents and visitors

Parents and visitors to the school will not be permitted to use the school's wifi unless specific authorisation is granted by the Headteacher.

The Headteacher will only grant authorisation if:

- Parents are working with the school in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the school's wifi 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 wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The Headteacher and governing body monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the school.

This policy will be reviewed every two years.

The Governing Board is responsible for approving this policy.

11. References

- [1] legislation.gov.uk, "Data Protection Act 2018," 2018. [Online]. Available: <http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted>. [Accessed 25 November 2022].
- [2] Information Commissioner's Office, "Guide to the UK General Data Protection Regulation (UK GDPR)," [Online]. Available: <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>. [Accessed 25 November 2022].

- [3] legislation.gov.uk, "Computer Misuse Act 1990," 1990. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1990/18/contents>. [Accessed 25 November 2022].
- [4] legislation.gov.uk, "Human Rights Act 1998," 1998. [Online]. Available: <https://www.legislation.gov.uk/ukpga/1998/42/contents>. [Accessed 25 November 2022].
- [5] legislation.gov.uk, "The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000," 2000. [Online]. Available: <https://www.legislation.gov.uk/uksi/2000/2699/regulation/3/made>. [Accessed 25 November 2022].
- [6] legislation.gov.uk, "Education Act 2011," [Online]. Available: <https://www.legislation.gov.uk/ukpga/2011/21/contents/enacted>. [Accessed 25 November 2022].
- [7] legislation.gov.uk, "Freedom of Information Act 2000," [Online]. Available: <https://www.legislation.gov.uk/ukpga/2000/36/contents>. [Accessed 25 November 2022].
- [8] legislation.gov.uk, "Education and Inspections Act 2006," 2006. [Online]. Available: <https://www.legislation.gov.uk/ukpga/2006/40/contents>. [Accessed 25 November 2022].
- [9] gov.uk, "Keeping children safe in education," [Online]. Available: <https://www.gov.uk/government/publications/keeping-children-safe-in-education--2>. [Accessed 25 November 2022].
- [10] gov.uk, "Searching, screening and confiscation at school," 13 July 2022. [Online]. Available: <https://www.gov.uk/government/publications/searching-screening-and-confiscation>. [Accessed 25 November 2022].
- [11] Alfred Lord Tennyson School, "Staff Disciplinary Policy," 2020.
- [12] Alfred Lord Tennyson School, "Staff Code of Conduct," 2020.
- [13] Alfred Lord Tennyson School, "Data Protection Policy".
- [14] Alfred Lord Tennyson School, "Child Protection and Safeguarding Policy".
- [15] Alfred Lord Tennyson School, "Online Safety Policy".
- [16] Alfred Lord Tennyson School, "ICT Acceptable Use Policy".

12. Safeguarding

Safeguarding our children is our priority – see Child Protection and Safeguarding Policy [14].

Online safety lessons are conducted regularly within the school to help to ensure that children stay safe online – see Online Safety Policy [15] and ICT Acceptable Use Policy [16].

All concerns must be reported to our Designated Safeguarding leads:
Mrs K O'Connor, Mrs S Smith, Mrs J Appleby and Mrs L Bunker

Never accept friend requests from pupils on social media

10 recommendation for school staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during school hours
7. Don't make comments about your job, your colleagues, our school or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the school on your profile (e.g. by setting it as your workplace, or by 'checking in' at a school event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list

Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts

The public may still be able to see posts you have **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster

Google your name to see what information about you is visible to the public

Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this

Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture

- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the Senior Leadership Team or the Headteacher about what's happening

A parent adds you on social media

It is at your discretion whether to respond. Bear in mind that:

- Responding to one parent's friend request or message might set an unwelcome precedent for both you and other teachers at the school
- Pupils may then have indirect access through their parent's account to anything you post, share, comment on or are tagged in

If you wish to decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2. Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers	
<p>Name of parent/carers:</p> <p>Name of child:.....</p>	
<p>Online channels are an important way for parents/carers to communicate with, or about, our school.</p> <ul style="list-style-type: none"> • The school uses the following channels: • Our official Facebook page <p>Email/text groups for parents (for school announcements and information)</p> <p>Our virtual learning platform – Purple Mash</p>	
<p>When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:</p> <ul style="list-style-type: none"> • Be respectful towards members of staff, and the school, at all times • Be respectful of other parents/carers and children • Direct any complaints or concerns through the school's official channels, so they can be dealt with in line with the school's complaints procedure <p>I will not:</p> <ul style="list-style-type: none"> • Use private groups, the school's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive and the school can't improve or address issues if they aren't raised in an appropriate way. I will contact the school and speak to the appropriate member of staff if I have any complaints or concerns. • Use private groups, the school's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the school and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident <p>Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers</p>	
<p>Signed:</p>	<p>Date:</p>

Appendix 3. Acceptable use agreements for pupils

Acceptable use of the school's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the school's ICT facilities (like computers and equipment) and get on the internet in school, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break school rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the school will check the websites I visit and how I use the school's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a school computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the school's ICT systems and internet.

I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (Parent/ Carer):

Date:

Acceptable use of the school's ipads: agreement for pupils

Name of pupil:

Staff and pupils must abide by all school rules with using the iPads.

Acceptable Use

The use of technology resources is a privilege, not a right. This acceptable use agreement is provided to make both staff and pupils aware of the responsibilities associated with efficient, ethical, and lawful use of technology resources. If you violate any of the User Terms and Conditions named in this agreement, privileges may be terminated and disciplinary action could be applied. When applicable, law enforcement agencies may be involved.

Staff and pupils are responsible for:

Using iPads in a responsible and ethical manner.

Obedying general school rules concerning behaviour and communication that apply to iPad/computer use.

Using all technology resources in an appropriate manner so as to not damage school equipment.

Complying with trademark and copyright laws and all license agreements. Ignorance of the law is not immunity. If you are unsure, ask a member of staff, Computing Subject Lead or Headteacher.

Network Connectivity

Staff and pupils are only allowed to access the school's network with the permission of a member of staff. If this is done without this permission, the staff/pupils will face discipline actions deemed appropriate by the administration.

Sound, Music, Games, or Apps

Sound must be muted at all times unless permission is obtained from the teacher.

Music is allowed on the iPad and can be used at the discretion of the teacher.

Non educational games are not allowed to be played on the iPads unless permission is obtained from the teacher. If permission is granted, these must be age appropriate and suitable for the school environment. If Teacher are unsure, please check with Computing Subject Lead, Technician or Headteacher.

Apps can be used at the discretion of the teacher. These apps need to be directly related to the curriculum and only downloaded through the Computing Subject Lead, Technician or Headteacher.

Screensavers/Background Photos

Screensavers and background photos are not to be changed! Inappropriate media may not be used as a screensaver or background photo.

Staff/Pupil Activities Strictly Prohibited

Illegal installation or transmission of copyrighted materials

Any action that violates existing school policy or public law

Sending, accessing, uploading, downloading, or distributing offensive and inappropriate material.

Internet Games which are not educational

Spamming-Sending mass or inappropriate emails

Gaining access to other user's accounts, files, and/or data

Vandalism- any malicious attempt to harm or destroy hardware, software or data

Signed (pupil):.....

Date:

Parent/carers agreement: I agree that my child can use the school's ICT systems and internet when appropriately supervised by a member of school staff. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (Parent/ Carer):

Date:

Appendix 4. Acceptable use agreement for staff, governors, volunteers and visitors

Acceptable use of the school's ICT facilities and the internet: agreement for staff, governors, volunteers and visitors

Name of staff member / governor / volunteer / visitor:

.....

When using the school's ICT facilities and accessing the internet in school, or outside school on a work device, 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 work devices are secure and password-protected when using them outside school, and keep all data securely stored in accordance with this policy and the school's data protection policy.

I will let the Designated Safeguarding Lead (DSL) and ICT manager 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 always use the school's ICT systems and internet responsibly, and ensure that pupils in my care do so too.

Signed:

(staff member / governor / volunteer / visitor)

.....

Equipment Loan Form for Staff

To be filled out by staff signing out the equipment.

Details of Loanee	
NAME OF STAFF MEMBER
ADDRESS
TELEPHONE NUMBER
EMAIL
Loan details	
LOAN DATE
DATE RETURNED
Equipment details	
TYPE [e.g. laptop/tablet]
MAKE [e.g. Acer/Lenovo/Apple]
MODEL
SERIAL NUMBER
ASSET NUMBER [insert number from your asset register]
EQUIPMENT CONDITION	

Loan details

[outline any significant defects/marks e.g. large scratch across screen]

Accessory details

DESCRIPTION [e.g. keyboard/mouse/laptop charger]

QUANTITY

LOANEE SIGNATURE:

.....

SCHOOL OFFICE MANAGER
AUTHORISATION SIGNATURE:

.....

Device Loan Agreements for Staff

This document should be read and signed in conjunction with the **Device Loan Form**. You should read the terms and conditions set out in the agreement and provide a signature at the end of this agreement to confirm that you have read and agree to these terms.

1. This agreement is between:

- 1) Alfred Lord Tennyson School, Rushden, Northamptonshire
- 2) [Insert staff member name and address]

And governs the use and care of devices assigned to individual staff members. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

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

The school is lending the employee [a laptop/tablet] for the purpose of [working from home/special project, etc]

This agreement sets the conditions for the employee taking the equipment home.

A **Device Loan Form** will be completed outlining the details of the device and equipment being loaned.

2. Damage/loss

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

I understand that I am responsible for the equipment at all times whether on the school's property or not.

If the equipment is **damaged, lost or stolen**, I will immediately inform the School Office Manager and I acknowledge that I am responsible for full replacement costs. If the equipment is stolen, I will also immediately inform the police and obtain a crime reference number.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I will not decorate or change the external face of the equipment provided in any way, including affixing stickers.

I will not leave the equipment unsupervised in unsecured areas.

I understand that all technical support and maintenance must go through Alfred Lord Tennyson School.

I will take reasonable health and safety precautions when using a device and I understand that the school is not responsible for any damage to person or property resulting from the device or equipment loaned.

3. Unacceptable use

I am aware that the school monitors my activity on the equipment.

I will not carry out any activity that constitutes 'unacceptable use'. This includes, but is not limited to:

- Accessing, creating, storing or linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Sharing confidential information about the school, its pupils, or other members of the school community
- Setting up any software, applications or web services on this device without approval by authorised personnel, or creating or using any programme, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Carrying out any activity which defames or disparages the school, or risks bringing the school into disrepute
- Using inappropriate or offensive language

I accept that if I engage in any activity that constitutes 'unacceptable use', I may face disciplinary action in line with the school's policies on Staff Discipline and the Staff Code of Conduct.

4. Personal use

I will be the sole user of this device and will not loan the equipment to any other person.

I will not install any software or equipment such as printers and scanners on to the device.

I will not make changes to the inner hardware.

I will not reset the laptop login password or add other accounts

I understand that the school is not responsible for any costs resulting from the use of the device and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.

I understand that there may be occasions when I need to return the device to school for upgrades and maintenance. I understand that because of these upgrades, it may be necessary to completely remove all information contained on the laptop and that Alfred Lord Tennyson School cannot be held responsible for the loss or damage of any data on the device during this process.

I understand that it is my responsibility to return the device to school and that during this process, technical members of staff may view data, website history or programmes on the device.

5. Data protection

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

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure the equipment locks if left inactive for a period of time

- 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 School Office Manager on the email bursar@alfredstreet.northants.sch.uk or Ross Smith from Interim IT on ross.smith@interim.co.uk

6. Return date

I will return the device in its original condition to the school office within 7 days of being requested to do so.

I will return the equipment to the school upon resignation, dismissal or if I leave the employment of the school for any other reason.

7. Consent

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

FULL NAME
SIGNATURE

Device Loan Agreements for Pupils

This document should be read and signed in conjunction with the Device Loan Form. You should read the terms and conditions set out in the agreement and provide a signature at the end of this agreement to confirm that you have read and agree to these terms.

1. This agreement is between:

- 1) Alfred Lord Tennyson School, Rushden, Northants
- 2) [Name of parent and their address]

and governs the use and care of devices assigned to the parent's child. This agreement covers the period from the date the device is issued through to the return date of the device to the school.

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

1. The school is lending the pupil [a laptop/tablet] for the purpose of doing schoolwork from home.
2. This agreement sets the conditions for taking an Alfred Lord Tennyson School laptop/tablet 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 whether on the school's property or not.

If the equipment is **damaged, lost or stolen**, I will immediately inform the **School Office Manager**, 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 and request a crime number.

I agree to keep the equipment in good condition and to return it to the school on their demand from the school in the same condition.

I agree to not leave the equipment unsupervised in unsecured areas.

I agree to keep the equipment in good condition and to return it to the school on demand from the school in the same condition.

I agree that the pupil will not decorate or change the external face of the equipment provided in any way, including affixing stickers.

I understand that all technical support and maintenance must go through Alfred Lord Tennyson School.

I will take reasonable health and safety precautions when using a device and I understand that the school is not responsible for any damage to person or property resulting from the device or equipment loaned.

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 am aware that the school monitors the pupil's activity on this device and that spot checks will be carried out on the device's search history.

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 the school, or risks bringing the school into disrepute
- Changing the security settings
- Causing intentional damage to ICT facilities or materials
- Using inappropriate or offensive language

I accept that the school will sanction the pupil, in line with our Behaviour Policy, if the pupil engages 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.

I agree that the pupil will not install any software or equipment such as printers and scanners on to the device.

I agree that changes to the inner hardware will not be made

I agree that the pupil will not reset the laptop login password or add other accounts

I agree that if homework is not completed the device must be returned

I understand that the school is not responsible for any costs resulting from the use of the device and the connectivity equipment, including electricity, printer cartridges, paper or any cost occurring from an internet service not provided by the school.

5. Data protection

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

- Keep the equipment password-protected - strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Make sure my child locks the equipment if it's left inactive for a period of time
- 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 the School Office Manager on the email **bursar@alfredstreet.northants-ecl.gov.uk**

6. Return date

I will return the device in its original condition to the **School Office** within **2 days** of being requested to do so.

I will ensure the return of the equipment to the school if the pupil no longer attends the school.

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

Equipment Loan Form for PUPILS

To be filled out by staff signing out the equipment.

Details of Pupil	
NAME
CLASS
YEAR GROUP
ADDRESS
PARENT'S TELEPHONE NUMBER
PARENT'S EMAIL
Loan details	
LOAN DATE
DATE RETURNED
Equipment details	
TYPE [e.g. laptop/tablet]
MAKE [e.g. Acer/Lenovo/Apple]
MODEL
SERIAL NUMBER

Loan detailsASSET NUMBER [insert number from
your asset register]

.....

EQUIPMENT CONDITION [outline any
significant defects/marks e.g. large
scratch across screen]

.....

Accessory details

DESCRIPTION

[e.g. keyboard/mouse/laptop charger]

QUANTITY

PARENT/CARER SIGNATURE:

.....

SCHOOL OFFICE MANAGER
AUTHORISATION SIGNATURE:

.....