The Talentum Learning Trust		Trust Policy Document			
Approved by:	**Trust Board**	**Issue date:**	**December 2023**	**Review date:**	**December 2025**
Policy Owner:	**CEO /DPO**	Page: **1 of 23**			
Audience:	**Trustees** ☑ **Staff** ☑ **Pupils** ☑ **Local Governing Bodies** ☑ **Parents** ☑ **General Public** ☑				

The Talentum Learning Trust ICT Policy

Contents

1. Purpose

Information technology (IT) is an integral part of the way The Talentum Learning Trust (TTLT) operates, and is a critical resource for pupils, staff, governors, volunteers and visitors. IT supports teaching and learning, pastoral support and the various business and administrative functions of TTLT and its schools.

The use of IT resources and systems also poses risks to data protection, online safety, and safeguarding, which need to be managed.

This policy aims to:

- Set guidelines and rules on the use of school ICT resources for staff, pupils, parents and governors
- Support policies on data protection, online safety and safeguarding
- Prevent disruption that could occur to the school through the misuse, or attempted misuse, of IT systems
- Support the school in teaching pupils safe and effective internet and IT use

This policy covers all users of our school's ICT facilities, including governors, staff, pupils, volunteers, contractors, and visitors.

Breaches of this policy may be dealt with under school behaviour policies, TTLT staff code of conduct, or TTLT disciplinary policies.

2. Definitions

IT systems: 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 TTLT IT service.

Users: anyone authorised by the school to use or access TTLT IT systems, including governors, staff, pupils, volunteers, contractors, and visitors

Personal use: any use or activity not directly related to the user's employment, study or purpose agreed by an authorised user.

Authorised personnel: employees authorised by TTLT to perform systems administration and/or monitoring of the IT systems.

Removable storage media: any storage device that is easily connected and disconnected from IT systems, including portable USB storage drives and SD cards.

TTLT IT Team: All ICT Managers and ICT technicians based centrally or at individual schools.

3. Related Policies and Legislation

This policy references or relates to the following other TTLT policies:

- GDPR policy
- Safeguarding policy – central staff
- Safeguarding policy - schools
- Staff code of conduct

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

- Data Protection Act 2018
- The UK General Data Protection Regulation (UK GDPR) – the EU GDPR was incorporated into UK legislation, with some amendments, by The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2020
- Computer Misuse Act 1990
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Education Act 2011
- Freedom of Information Act 2000
- Education and Inspections Act 2006
- Keeping Children Safe in Education 2022
- National Cyber Security Centre (NCSC): Cyber Security for Schools
- Education and Training (Welfare of Children) Act 2021
- Meeting digital and technology standards in schools and colleges

4. Email Usage Principles

TTLT provides each member of staff with an email account. This email account should be used for work purposes only.

The Talentum Learning Trust shall reserve the right to purge identifiable personal email to preserve the integrity of the email systems.

No employee or student shall send, forward or receive emails that in any way may be interpreted as insulting, disruptive or offensive by any other person, or company. Examples of prohibited material include but are not limited to:

- Sexually explicit messages, images, cartoons, jokes or movie files
- Unwelcome propositions
- Profanity, obscenity, slander or libel
- Ethnic, religious or racial slurs
- Political beliefs or commentary
- Any message which could be viewed as harassment or disparagement of others based on their sex, race, sexual orientation, age, national origin, disability or religious or political beliefs.

The Talentum Learning Trust owns the e-mail system which means that all email traffic, both sent and received, including attachments, shall be monitored, and reviewed and any action deemed appropriate shall be taken.

This means that nothing should be taken to be private, even if marked as “private” and/or “confidential” or with any similar wording.

This monitoring will make sure that this policy is effective and that users of the email system are abiding by its content. The monitoring is also to ensure that the Talentum Learning Trust email system(s) are working properly.

All staff and students shall ensure compliance with relevant legislation.

Email folders shall be reviewed regularly, and any non-essential messages shall be deleted.

A standard footer should be appended to all external email messages:

- Limiting liability and including an appropriate disclaimer
- Detailing the Talentum Learning Trust establishment’s registered address

Internal email and other internal information shall not be forwarded to destinations outside of the Trust domain(s) without the authority of the appropriate individual.

Email users shall not forward chain letters either internally or externally. This includes those purporting to be for charity or other good causes as well as those promising wealth or other personal gain. Virus warnings shall come under the same exclusion, as the majority of these are false. Staff should refer to the TTLT IT team to check the validity of such messages but shall not forward these messages to anyone inside or outside the Trust under any circumstances.

Emails of any kind shall not be sent to multiple external organisations without the appropriate approval of a senior staff member. This may be considered as ‘spamming’ which is an illegal activity in some countries.

The individual logged in at a computer shall be considered to be the author of any messages sent from that computer. All ICT users shall log off or lock their computers when away from their desks; under no circumstances should a user send a message from somebody else's account.

Email addresses should not be disclosed unnecessarily. Information provided in surveys or other questionnaires may lead to risks such as receiving unwanted junk messages.

Email communications to multiple recipients outside of the organisation should be 'blind carbon copied' (bcc) to protect personal data, in line with GDPR requirements.

Email shall not be used to send large, attached files, unless very urgent and authorised by the TTLT IT Team. The email system has a 10MB capacity and if returned, large files may result in overloading the email system.

Emails and attachments shall not be opened unless they are from a known source. Caution shall also be exercised even if attachments are received from a known source but are unexpected.

The facility to automatically forward emails shall not be used to forward messages to personal email accounts.

Emails may be archived by ICT Support to meet both the Learning Trusts requirements and any legal obligations.

5. Social Media

The Trust understands that social media is a growing part of life. Staff have a responsibility to safeguard pupils against potential dangers when accessing the internet and to educate pupils about how to protect themselves online when outside of school.

The Trust is committed to:

- Encouraging the responsible use of social media by all staff, parents, and pupils in support of the Trust's mission, values and objectives.
- Protecting our pupils from the dangers of social media.
- Preventing and avoiding damage to the reputation of the Trust and its schools through irresponsible use of social media.
- Protecting our staff from cyber bullying and potentially career damaging behaviour.
- Meeting the digital and technology standards in schools and colleges

School accounts:

School social media passwords are kept secure – these are not shared with any unauthorised persons, unless otherwise permitted by the Headteacher.

Only appropriately trained staff shall have access rights to school social media platforms.

Staff will ensure any posts are positive in nature and relevant to pupils, the work of staff, the Trust, school, or any achievements.

Staff will always adhere to the principles of UK GDPR.

Staff will not post any content online which is damaging to the Trust, school or any of its staff or pupils.

If inappropriate content is accessed online, a report form will be completed and passed on to the Headteacher. The Headteacher retains the right to monitor staff members' internet usage in line with the TTLT Data and Cyber-Security Breach Prevention and Management Plan.

Personal accounts:
Staff members will not access social media platforms during lesson times.

Staff members will not use any school-owned devices to access personal accounts, unless it is beneficial to the material being taught. Prior permission must be sought from the Headteacher.

Staff members are permitted to use social media during break times, but only on personal devices.

Staff are not permitted to use the school's WiFi network to access personal accounts, unless otherwise permitted by the Headteacher, and once the TTLT IT team has ensured the necessary network security controls are applied.

Staff will avoid using social media in front of pupils.

In line with the staff code of conduct, staff will not "friend" or otherwise contact pupils or parents through their personal social media accounts.

If pupils or parents attempt to "friend" a staff member they will report this to the Headteacher.

Staff members will not provide their home address, phone number, mobile number, social networking details or email addresses to pupils or parents – any contact with pupils or parents will be done through authorised school contact channels.

Staff members will ensure the necessary privacy controls are applied to personal accounts.

Staff members will avoid identifying themselves as an employee of the Trust on their personal social media accounts.
Staff members will not post any content online that is damaging to the school, Trust or any of its staff or pupils.

Where staff members use social media in a personal capacity, they will ensure it is clear that views are personal and are not that of the Trust.

Staff members will not post any information which could identify a pupil, class, school or Trust – this includes any images, videos and personal information.

Staff will not take any posts, images or videos from social media that belong to the Trust for their own personal use.

Staff members will not post anonymously or under an alias to evade the guidance given in this policy.

Breaches of this policy by members of staff will be taken seriously, and in the event of illegal, defamatory, or discriminatory content, could lead to prosecution, disciplinary action, or dismissal.

Members of staff will be aware that if their out-of-work activity brings the Trust into disrepute, disciplinary action will be taken.

Members of staff are encouraged to regularly check their online presence for negative content via search engines.

Attempts to bully, coerce, or manipulate members of the school community via social media by members of staff will be dealt with as a disciplinary matter.

Staff members will use their school email address for school business and personal email address for their private correspondence; the two should not be mixed.

Social media use – pupils and parents:
Pupils will not access social media during lesson time unless it is part of a curriculum activity.

Pupils and parents will not attempt to "friend" or otherwise contact members of staff through their personal social media accounts. Pupils and parents are only permitted to be affiliates of school social media accounts.

Where a pupil or parent attempts to "friend" a staff member on their personal account, it will be reported to the Headteacher.

Pupils and parents will not post anonymously or under an alias to evade the guidance given in this policy.

Pupils and parents will not post any content online which is damaging to the school, Trust or any of its staff or pupils.

Pupils are instructed not to sign up to any social media sites that have an age restriction above the pupil's age.

If inappropriate content is accessed online on school premises, it will be reported to a teacher.

Pupils are not permitted to use the school's WiFi network to access any social media platforms unless prior permission has been sought from the Headteacher, and the TTLT IT Team has ensured appropriate network security measures are applied.

Parents are not permitted to use the school's WiFi network to access any social media platforms on personal devices.

Breaches of this policy will be taken seriously, and in the event of illegal, defamatory, or discriminatory content could lead to prosecution, or exclusion.

6. Acceptable Use of IT – Staff, including governors, directors, visitors, volunteers, and contractors.

Access to TTLT IT systems is provided for, and must only be used for, work purposes.

Staff must only use their own accounts to access TTLT IT systems. Staff must keep the credentials for such accounts (e.g. passwords) secret.

Staff must not allow anyone else to use their access to TTLT IT systems, including when leaving equipment or systems unattended.

Staff should enable multi-factor authentication on their accounts where systems allow for this. The TTLT IT team may enforce multi-factor authentication and / or additional security measures as required.

TTLT provides each member of staff with an email account. This email account should be used for work purposes only.

Staff must ensure that their use of TTLT IT systems is in line with the staff code of conduct.

Staff may not use TTLT IT systems for personal use.

Staff must follow guidance from the TTLT IT team on how to store data and files in the appropriate systems and locations.

Staff must not connect removable storage media to TTLT IT systems without explicit approval from the TTLT IT team. Such requests will only be granted under exceptional circumstances.

Where remote access is provided to TTLT IT systems, staff must abide by the same rules as apply when accessing systems on site.

Staff must be particularly vigilant if they use the school's ICT facilities outside the school and take such precautions as the TTLT IT team may require 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.

Staff will sign the Acceptable Use Agreement up on commencement of employment and on an annual basis. See Appendix 1.

6. Acceptable Use of IT - Students

Schools should use the TTLT template policy for student access to IT systems. The template Acceptable Use Agreement is included at Appendix 2 to this policy. For Primary aged pupils, a pupil friendly template has been provided in Appendix 3.

7. Acceptable Use of IT - Parents

Parents should not have access to the Trust's ICT facilities as a matter of course. However, parents working for, or with, the Trust 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 Trust's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy, as well as the associated policies listed in section 3, as they apply to staff.

8. IT equipment

All IT equipment must be recorded on the TTLT asset register. Each school holds an ICT Asset register.

Staff may be issued with laptops, phones, monitors, or other IT equipment to allow them to carry out their role.

The TTLT IT team will manage the assignment of devices to staff. The ICT Asset register will be kept updated when devices are assigned to staff.

Staff must sign a device agreement for all equipment that they are assigned. A template device agreement can be found in Appendix 4.

Staff must take reasonable care of loan equipment, taking good care of the physical condition of the equipment. Staff may be required to pay for repairs where there is evidence they have been negligent in their use and care of issued equipment.

Staff must ensure that all loan equipment is stored securely when not in use, including when taking devices away from TTLT premises.

Staff must not remove IT equipment from its assigned location without permission from the TTLT IT team.

There may be occasions when pupils are permitted access to Trust devices off site. The Trust has delegated the responsibility of allocating devices to Headteachers. A template for borrowing IT equipment has been provided, see Appendix 5.

Fixed IT equipment (e.g. desktop computers, printers, photocopiers, servers, networking equipment) may not be moved, altered, or otherwise changed without approval from the TTLT IT team.

All networking, server, storage, or other infrastructure equipment must be stored in a secure location, only accessible to the TTLT IT team and delegated keyholders.

9. Personal devices

Staff are permitted at their discretion, to access TTLT IT systems and services from personal devices. When using personal devices on TTLT IT systems, staff must ensure that such usage is in line with this section.

All personal devices used to access TTLT IT systems must be up to date with the latest security patches, up-to-date anti-virus, running a currently supported operating system, and protected by strong encryption and passwords.

The TTLT IT services team may implement policies to enforce compliance with security requirements for personal devices and prevent access from devices that do not pass these checks.

TTLT may require staff to grant limited access to manage personal devices when using them to access TTLT IT systems.

TTLT may suspend or remove access to TTLT systems from personal devices at any time.

TTLT reserves the right to automatically remove work data from personal devices at the end of a member of staff's employment.

TTLT reserves the right to remove work data from personal devices in order to prevent, mitigate or otherwise address a data breach, cyber security risk, or policy breach.

For the purposes of intellectual property any data held on personal devices is the property of TTLT.

For the purposes of GDPR TTLT is the data controller for any TTLT data held on personal devices. TTLT data is any that relates to the individual's work as an employee of TTLT. This data is disclosable under Freedom of Information and Subject Access Requests.

10. Monitoring

To safeguard and promote the welfare of children and provide them with a safe environment to learn, TTLT reserves the right to filter and monitor the use of its ICT systems, services, and equipment.

Monitoring includes, but is not limited to, the filtering and monitoring of Internet activity, bandwidth usage, user activity, access and audit logs, telemetry data and any other electronic communications.

Only authorised IT or safeguarding personnel may filter, inspect, monitor, intercept, assess, record, and disclose the above, to the extent permitted by law.

The effectiveness of any filtering and monitoring will be regularly reviewed by the Headteachers, DSL's, DPO and TTLT IT team.

Where appropriate, authorised personnel may raise concerns about monitored activity with the school's Designated Safeguarding Lead (DSL) and the TTLT IT team or through TTLT's Whistleblowing Policy.

11. Data Security

Individual schools are responsible for making sure appropriate levels of security protection and procedures are in place to safeguard its systems, staff, and pupils.

Schools must take steps to protect the security of all computing resources, data, and user accounts. The effectiveness of these procedures will be reviewed periodically by the Headteachers, DSL's, DPO

and TTLT IT team to ensure security is sufficient to protect the school from evolving cyber-crime technologies.

Staff, pupils, parents and other who use the TTLT IT facilities should use safe computing practices at all times.

TTLT aims to meet the cyber security standards recommended by the DfE's guidance on digital and technology standards in schools and colleges.

All users of TTLT IT systems should set strong passwords for their accounts and keep these passwords secure. The Trust implements Microsoft's password policy for network and email access.

Passwords should:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least six characters in length
- Contain characters from three of the following four categories:
- English uppercase characters (A through Z)
- English lowercase characters (a through z)
- Base 10 digits (0 through 9)
- Non-alphabetic characters (for example, !, $, #, %)
- Complexity requirements are enforced when passwords are changed or created.

Passwords should NOT be:

- written down
- easy to guess
- shared with any other people including family and friends.

In line with the National Cyber Security Centre's password guidance, the Trust recommends staff use the 'three random words' policy for all other systems.

Users are responsible for the security of their passwords and accounts, and for setting permissions for files they control.

Members of staff or pupils who disclose account or password information may be subject to disciplinary action. Parents, visitors, or volunteers who disclose account or password information may have their access rights revoked.

If users suspect that their password has been shared or discovered, they must change it immediately. If users suspect that their account may have been accessed by anyone else, they must change their password immediately and then contact the TTLT IT team.

The TTLT IT team ensures that all TTLT devices and systems are protected by an appropriate level of encryption.

Trust 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 or TTLT IT team.

Use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption.

12. Cyber Security

TTLT understands the importance of cyber security and will ensure cyber security is given the time and resource needed to keep the trust and its schools secure.

TTLT will endeavour to meet the Cyber Security Standards detailed in the Dfe published digital and technology standards in schools and colleges.

TTLT will provide annual training for staff on the basics of cyber security.

TTLT and its schools will make sure staff are aware of the correct procedures for reporting and responding to cyber security incidents.

Details on how report cyber incidents are included in the Data and Cyber-security Breach Prevention and Management Plan.

TTLT will keep backups of key systems and data according to an appropriate schedule based on risk.

The TTLT IT team will manage and monitor the backup systems, report, and address faults, and keep records of such checks and remediation actions.

TTLT will develop, review, and test a Data and Cyber-security Breach Prevention and Management Plan. This plan will be activated in the event of a cyber security incident and will be updated as needed following incident reviews.

TTLT will take steps to check the security of supplier IT systems when procuring or renewing systems, goods, or services. This responsibility may be delegated to schools, depending on the system requirements.

13. Network and Internet access

Where TTLT procures network and internet access to school sites for staff, students, visitors, and others as required for their role; such access is provided and to be used in accordance with the following:

TTLT Internet connections must be secured by a suitable firewall and filtering solution.

Changes to filtering must be logged, approved, and implemented in line with the Dfe guidance on filtering and monitoring standards, detailed in the digital and technology standards in schools and colleges.

Changes to filtering must be approved by the Headteacher and TTLT IT Team. The undertaking of the change may be delegated third-party broadband filtering providers. In this instance, authorisation must be sought from appropriate staff prior to requesting the change.

Staff must report any sites they believe are inappropriate that have not been correctly identified and blocked by the filtering systems to the TTLT IT team or external provider where appropriate. See Appendix 4.

Staff should report any sites they believe have been incorrectly blocked by the filtering systems to the TTLT IT team or external provider where appropriate. See Appendix 4.

Any attempts to bypass TTLT firewalls or web filtering may result in disciplinary action.

14. Changes to TTLT IT systems

Any changes to TTLT IT systems must be managed and approved by the Central Executive Team.

Any unauthorised changes to TTLT IT systems may result in disciplinary action.

Appendix 1: Staff acceptable use agreement

Name:	

I have read and understood the full TTLT IT Policy and Acceptable Use Statement and agree to uphold the spirit and the letter of the approaches outlined there.

I will ensure that my use of IT systems is conducted in line with this policy, and I will take all reasonable steps to ensure the security and safety of the IT systems I have access to, and any equipment that is loaned to me.

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 TTLT GDPR policy.

I understand that TTLT may monitor the websites I visit, and my use of IT systems.

I will only use my own accounts to access TTLT IT systems. I will set secure passwords and I will not share my passwords with anyone else.

I will always use the school's ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed:	**Date:**

Appendix 2: Model pupil acceptable use agreement

Name of pupil:	

When I use the school's IT systems (like computers and equipment) and go 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
- Send any photos, videos or livestreams of people (including me) who aren't wearing all of their clothes
- 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:**

Appendix 3: Model Child-friendly acceptable use agreement

We know that it can be fun to use technology as part of your learning experience. We want everyone to be able to use technology, like computers and tablets, but it is important that you are safe when you are using them.

We have created this agreement to help you understand how to be safe when you are using technology. Please read this carefully and sign your name to show that you understand your responsibilities when using technology. Ask your teacher if there is something that you do not understand.

I will:

- ✓ Only use technology, such as a computer, when a teacher has given me permission.
- ✓ Only use technology for the reason I have been asked to use it.
- ✓ Only use the internet when a teacher has given me permission.
- ✓ Ask for help when I have a problem using the technology.
- ✓ Look after the device and try not to damage it.
- ✓ Tell the teacher if my device is not working or damaged.
- ✓ Tell the teacher if I think someone else is not using technology safely or correctly.
- ✓ Tell the teacher if I see something online that I think is inappropriate or that makes me upset.

I will not:

- ✘ Tell another pupil my username and password.
- ✘ Share personal information, such as my age and where I live, about myself or my friends online.
- ✘ Access social media, such as Facebook and WhatsApp.
- ✘ Speak to strangers on the internet.
- ✘ Take photos of myself or my friends using a school device.

Please read each statement and provide a tick to show that you agree, and then write your name below.

- ☐ I understand why it is important to use technology safely and correctly.
- ☐ I understand my responsibilities when using technology.
- ☐ I understand that I may not be allowed to use technology if I do not use it safely and correctly.
- ☐ I will follow these rules at all times.

Pupil name (please print): _____

Date: _____

Parent name (please print): _____

Parent signature: _____

Date: _____

Appendix 4: Model Template Devices user agreement – staff

This agreement is between (SCHOOL NAME) and (staff name) _____ and is valid for the academic year of _____.

XXX School has created this agreement to ensure that the above named member of staff understands their responsibilities when using school-owned devices, such as mobile phones and tablets, whether on or off the school premises.

Please read this document carefully, ensuring you understand what is expected, and sign below to show you agree to the terms outlined.

The school

XXXX School retains sole right of possession of any school-owned device and may transfer the device to another teacher if you do not, or are unable to, for any reason, fulfil the requirements of this agreement.

Under this agreement, the school will:

- Provide devices for your sole use while you are a permanent full-time or part-time teacher at the school.
- Ensure devices are set up to enable you to connect to, and make effective use of, the school network.
- Ensure the relevant persons, such as the ICT technician, have installed the necessary security measures on any school-owned device before your use – including, but not limited to, the following:
  - Firewalls
  - Malware protection
  - User privileges
  - Filtering systems
  - Password protection and encryption
  - Mail security technology
  - Tracking technology
- Ensure that all devices undergo the following regular checks and updates by the ICT technician, in line with school policy:
  - Termly updates to malware protection
  - Termly software updates
  - Annual password re-set requirements
  - Termly checks to detect any unchanged default passwords
  - Malware scans in line with specific requirements

- Plan and manage the integration of devices into the school environment, and provide the professional development required to enable you to use the devices safely and effectively.

- When required, expect you to pay an excess for accidental damage or loss repair/replacement costs, where loss or damage is a result of your own negligence.

Under this agreement, you will:

Overall use and care

- Bring the device and charging unit to the school each day and keep the device with you, or within your sight, at all times.
- Transport the device safely using the cover and carry case, if necessary, issued with the device.
- Not permit any other individual to use the device without your supervision, unless agreed by the Headteacher.
- Take responsibility for any other individual using the device.
- Provide suitable care for the device at all times and not do anything that would permanently alter it in any way.
- Lock the device screen when not in use with a passcode.
- Keep the device clean.
- Store devices in a lockable cupboard located in the staffroom or classroom during lesson times.
- Ensure all devices are switched off or set to silent mode during school hours.
- Immediately report any damage or loss of the device to the ICT technician.
- Ensure any tracking technology applied is active at all times.
- Immediately report any viruses or reduced functionality following a download or access to a site, to the ICT technician.
- Be prepared to cover the insurance excess, repair or replacement of the device when the damage or loss has been a result of your own negligence.
- Make arrangements for the return of the device and passcode to the ICT technician if your employment ends or if you will be away from the school for more than one week.

Using devices

- Only use the devices that have been permitted for your use by the Headteacher.
- Only use devices for educational purposes.
- Only use apps that are GDPR-compliant and from reputable sources.
- Ensure that any personal data is stored in line with the GDPR.
- Only store sensitive personal data on your device where absolutely necessary and which is encrypted.
- Ensure any school data stored on a device is encrypted and pseudonymised.
- Give permission for the ICT technician to erase and wipe data off your device if it is lost, or as part of exit procedures.
- Obtain permission prior to accessing learning materials from unapproved sources.
- Not search for, view, download, upload or transmit any explicit or inappropriate material when using the internet.
- Not share any passwords with pupils, staff or third parties unless permission has been sought from the Headteacher.

- Not install any software onto your device unless instructed to do so by the ICT technician or Headteacher.
- Ensure your device is protected by anti-virus software installed by the ICT technician and that this is checked on a weekly basis.
- Not use your device to take images or videos of pupils, staff or parents unless permission has been granted from the Headteacher.
- Not store any images or videos of pupils, staff or parents on your device unless consent has been sought from the individual(s) in the images or videos.
- In line with the above, only process images or videos of pupils, staff or parents for the activities for which consent has been sought.
- Not use your device to communicate with pupils or parents, unless permission has been sought from the Headteacher.
- Not use your device to send any inappropriate messages, images or recordings.
- Ensure that your device does not contain inappropriate or illegal content.
- Only access social media sites as approved by the Headteacher on your device, and ensure they are used in accordance with the Technology Acceptable Use Agreement.
- Allow the ICT technician to monitor your usage of your device, such as internet access, and understand the consequences if you breach the terms of this agreement.

Insurance cover provides protection from the standard risks whilst the device is on the school premises or in your home but excludes theft from your car or other establishments. Should you leave the device unattended and it is stolen, you will be responsible for its replacement and may need to claim this from your insurance company or pay yourself.

Failure to agree to, or abide by, these terms will lead to the device being returned to the school and serious breaches may result in disciplinary action.

I certify that I have read and understood this agreement and ensure that I will abide by each principle.

Signed: Date:

Print name: Device model and number:

(Headteacher)

Signed: Date:

Print name:

Appendix 5: Model Borrowing IT Equipment Agreement - Parents/Pupils

This agreement is between **name of school** and parents whose children are borrowing school IT equipment, and is valid from **date** to **date**.

Or:

This agreement is between **name of school** and **name of pupil** who will be borrowing school IT equipment, and is valid from **date** to **date**.

The device is the property of the school and activity can be monitored for any breaches of the school's **Acceptable Use Agreement**

We have created this agreement to ensure you understand your responsibilities as a parent whilst your child is borrowing IT equipment from the school.

Or:

We have created this agreement to ensure you understand your responsibilities whilst you are borrowing IT equipment from the school.

Responsibilities

- You must ensure you/your child treats the device in line with the school's **Acceptable Use Agreement** – the school has provided parents with this via **email**.
- You must ensure that the device is not used for any personal reasons by you/your child
- You must ensure nobody but you/your child has access to the device.
- You must ensure the device is stored safely.
- You must make sure the device is not used near any food or drink.
- If you/your child leaves the school before completing the school year, you must return the device to the school.
- If you/your child is excluded from the school, you must return the device to school.
- If the device is lost stolen, you must report it to the school and the police immediately.
- If the device is damaged, you must report it to the school immediately.
- If covers, chargers, or other equipment for the device are damaged whilst it is in your / child's possession, you must pay for a replacement or repair costs.
- If the device is damaged whilst it is in your / child's possession, you must pay for the replacement or repair costs.
- You must ensure you/your child understands their responsibilities for looking after the device, as outlined in this agreement – this must be signed and returned before the school releases any IT equipment on loan.
- You must ensure any software damage, e.g., viruses are reported to the school immediately.

- You must ensure that no applications are disabled on the device and make sure the device is not modified in any way or synced with another device.
- You and your child must have due regard to the school's **ICT Policy** – the school has provided parents with this via **email**.

Please read each statement and provide a tick to show you agree to the terms, then provide your name below. This must be returned to **name** via **email**.

- ☐ I will carry out my responsibilities as outlined in this agreement.
- ☐ I will ensure my child has read and signed the **IT Equipment User Agreement - Pupils**.
- ☐ I understand that I must pay for any loss or damage to either the device or any equipment for the device.

Parent name (please print): _____

Parent signature: _____

Date: _____

Pupil name (please print): _____

Pupil signature: _____

Date: _____