Staff and Visitor Acceptable Use Policy & Agreement

Table of Contents

Policy Document number: *FPS-POL-AUP-004*
Body reviewed and approved by: *Teaching & Learning Committee*
Date adopted: *New Policy Adopted September 2025*
Date for review: *September 2026*
Other information: *Based on model policy produced by The School Bus, last reviewed by The School Bus August 2022*

Acceptable Use Policy & Agreement

Introduction

Fulbourn Primary School believes that ICT plays an important part in both teaching and learning over a range of subjects, and the school accepts that both school-owned and personal electronic devices are widely used by members of staff. The school is committed to ensuring that both staff and pupils have access to the necessary facilities and support to allow them to carry out their work. The online world is now integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

The school has a sensible and practical approach that acknowledges the use of devices, and this policy is intended to ensure that:

- Members of staff and volunteers are responsible users and remain safe while using the internet and other communications technologies for education, personal and recreational use.
- School ICT systems and users are protected from accidental or deliberate misuse which could put the security of the systems and/or users at risk.
- Members of staff are protected from potential risks in their everyday use of electronic devices.

The school will try to ensure that staff and volunteers have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Personal use of ICT equipment and personal devices is permitted at the school; however, this is strictly regulated and must be done in accordance with this policy, and the Social Media Policy.

1 Legal Framework

This policy has due regard to all relevant legislation and statutory guidance including, but not limited to, the following:

- Data Protection Act 2018
- Computer Misuse Act 1990
- Communications Act 2003
- Freedom of Information Act 2000
- Human Rights Act 1998
- Voyeurism (Offences) Act 2019
- The UK General Data Protection Regulation (UK GDPR)
- Keeping Children Safe in Education
- Guidance for Safer Working Practice for those Working with Children and Young People

This policy operates in conjunction with the following school policies:

- Safeguarding and Child Protection
- Data Protection Policy
- Use of Mobile Phones and other Smart Devices Policy
- Complaints Procedures Policy
- Code of Conduct for all Adults
- Disciplinary Policy and Procedure
- Social Media Policy

2. Roles and Responsibilities

The governing board has the responsibility for the overall implementation of this policy, ensuring it remains compliant with relevant legislation.

The headteacher is responsible for:

- Reviewing and amending this policy, taking into account new legislation, government guidance and previously reported incidents, to improve procedures.
- The day-to-day implementation and management of the policy.
- The overall allocation and provision of resources.
- Handling complaints regarding this policy as outlined in the school's Complaints Procedures Policy.
- Informing staff that the school reserves the right to access personal devices for the purpose of ensuring the effectiveness of this policy.
- Ensuring that all school-owned and personal electronic devices have security software installed, to protect sensitive data in cases of loss or theft.
- Ensuring that all school-owned devices are secured and encrypted in line with the school's Data Protection Policy.
- Ensuring that all devices connected to the school network and internet are encrypted.
- Ensuring all staff are aware of, and comply with, the data protection principles outlined in the school's Data Protection Policy.

The Online Safety Lead is responsible for:

- Carrying out checks on internet activity of all user accounts and to report any inappropriate use to the headteacher.
- Monitoring the computer logs on the school's network and to report any logged inappropriate use to the headteacher.

The ICT Service/Technician is responsible for:

- Remotely viewing or interacting with any of the computers on the school's network. This may be done randomly to implement this policy and to assist in any difficulties.

- Ensuring routine security checks are carried out on all school-owned and personal devices that are used for work purposes to check that appropriate security measures and software have been updated and installed.
- Accessing files and data to solve problems for a user, with their authorisation.
- Adjusting access rights and security privileges in the interest of the protection of the school's data, information, network and computers.
- Disabling user accounts of staff who do not follow this policy, at the request of the headteacher.
- Assisting the headteacher in all matters requiring reconfiguration of security and access rights and in all matters relating to this policy.
- Assisting staff with authorised use of the ICT facilities and devices, if required.
- Immediately reporting any breach of personal devices to the DPO

Staff members are responsible for:

- Requesting permission from the headteacher or ICT technician, subject to their approval, before using school-owned devices for personal reasons during school hours.
- Requesting permission to assign school equipment and devices from the headteacher.
- Requesting permission from the headteacher, subject to their approval, before using personal devices during school hours and ensuring these devices are submitted for security checks when requested.
- Ensuring any personal devices that are connected to the school network are encrypted in a manner approved by the school.
- Reporting misuse of ICT facilities or devices, by staff or pupils, to the headteacher.
- Reading and signing an Acceptable Use Agreement and Device User Agreement to confirm they understand their responsibilities and what is expected of them when they use school-owned and personal devices.

The SBM is responsible for:

- Maintaining a Fixed Asset Register to record and monitor the school's assets.
- Ensuring value for money is secured when purchasing electronic devices.
- Monitoring purchases made under the Finance Policy.
- Overseeing purchase requests for electronic devices.

3. Classifications

School-owned and personal devices or ICT facilities include, but are not limited to, the following:

- Computers, laptops and software
- Monitors
- Keyboards

- Mouses
- Scanners
- Cameras
- Camcorders
- Other devices including furnishings and fittings used with them
- Mail systems (internal and external)
- Internet and intranet (email, web access and video conferencing)
- Telephones (fixed and mobile)
- Tablets and other portable devices
- Computers
- Photocopying, printing and reproduction equipment
- Recording and playback equipment
- Documents and publications (any type of format)

4. Acceptable Use

This policy applies to any computer or other device connected to the school's network and computers.

The school will monitor the use of all ICT facilities and electronic devices. Members of staff will only use school-owned and approved personal devices for work duties and educational purposes. The duties for which use is permitted include, but are not limited to, the following:

- Preparing work for lessons, activities, meetings, reviews, etc.
- Researching any school-related task
- Any school encouraged tuition or educational use
- Collating or processing information for school business
- Communicating with other members of staff, such as contacting the school office for assistance.

Inappropriate use of school-owned and personal devices could result in a breach of the school's Data Protection Policy.

Inappropriate use of school-owned and personal devices could result in a breach of legislation, including the UK GDPR and Data Protection Act 2018.

Any member of staff found to have breached the school's Data Protection Policy or relevant legislation will face disciplinary action.

Staff will always be an example of good practice to pupils, serving as a positive role model in the use of ICT and related equipment.

Since ICT facilities are also used by pupils, the school will have acceptable use agreements in place for pupils – staff will ensure that pupils comply with these.

Pupils found to have been misusing the ICT facilities will be reported to the headteacher.

School-owned electronic devices will not be used to access any material which is illegal, inappropriate, or may cause harm or distress to others.

Any illegal, inappropriate or harmful activity will be immediately reported to the headteacher.

Members of staff will not:

- Open email attachments from unknown sources.
- Use programmes or software that may allow them to bypass the filtering or security systems.
- Upload or download large capacity files without permission from the Headteacher.
- Give their home address, phone number, social networking details or email addresses to pupils or parents – contact with parents will be done through authorised school contact channels.

All data will be stored appropriately in accordance with the school's Data Protection Policy.

Members of staff will only use school-owned electronic devices to take pictures or videos of people who have given their consent.

School-owned electronic devices will not be used to access personal social media accounts.

Personal electronic devices will not be used to communicate with pupils or parents, including via social media.

Staff will ensure they:

- Express neutral opinions when representing the school online.
- Avoid disclosing any confidential information or comments regarding the school, or any information that may affect its reputability.
- Have the necessary privacy settings are applied to any social networking sites.

Images or videos of pupils, staff or parents will only be published online for the activities which consent has been sought.

Copyrighted material will not be downloaded or distributed.

School-owned devices will be taken home for work purposes only. Remote access to the school network will be given to staff using these devices at home.

School equipment that is used outside the premises, e.g. laptops, will be returned to the school when the employee leaves employment, or if requested to do so by the headteacher.

While there is scope for staff to utilise school equipment for personal reasons, this will not be done during working hours unless approved by the headteacher or in the case of a personal emergency.

Private business will not be mixed with official duties, e.g. work email addresses will be reserved strictly for work-based contacts only.

Use of a school-owned phone for personal use will be permitted for necessary calls.

Personal use of school-owned equipment can be denied by the headteacher at any time. This will typically be because of improper use or over-use of school facilities for personal reasons. A charge may be made for using equipment if the values are significant.

Where permission has been given to use the school equipment for personal reasons, this use will take place during the employee's own time, e.g. during lunchtime or after school. Where this is not possible, or in the case of an emergency, equipment can be used for personal reasons during work hours provided that disruption to the staff member's work, and the work of others, is minimal.

Abuse of ICT facilities or devices could result in privileges being removed. Staff will be aware of acceptable ICT use, and misuse of the facilities, as defined in this policy, will be reported to the headteacher.

Failure to adhere to the rules described in this policy may result in disciplinary action, in line with the Disciplinary Policy and Procedure.

5. Emails and the Internet

The school email system and internet connection are available for communication and use on matters directly concerned with school business.

Emails will not be used as a substitute for face-to-face communication, unless it is otherwise impossible.

Unprofessional messages will not be tolerated. All emails will be written in a professional tone and will be proof read by the staff member sending the email to ensure this prior to sending.

Abusive messages will not be tolerated – any instant of abuse may result in disciplinary action.

If any email contains confidential information, the user will ensure that the necessary steps are taken to protect confidentiality.

The school will be liable for any defamatory information circulated either within the school or to external contacts.

The school email system and accounts will never be registered or subscribed to spam or other non-work-related updates, advertisements or other personal communications. School email addresses will not be shared without confirming that they will not be subjected to spam or sold on to marketing companies.

All emails that are sent or received will be retained in accordance with the Records Management Policy. The timeframe will be altered where an inbox becomes full.

The types of information sent through emails to a personal device will be limited to ensure the protection of personal data, e.g. pupils' details.

Contracts sent via email or the internet are as legally binding as those sent on paper. An exchange of emails can lead to a contract being formed between the sender, or the school, and the recipient. Staff will never commit the school to any obligations by email or the internet without ensuring that they have the authority to do so.

Any suspicious emails will be recorded in the incident log and will be reported to the headteacher. All incidents will be responded to in accordance with the Online Safety Policy.

6. Portable Equipment

All data on school-owned equipment is synchronised with the school cloud-based storage system or on the school's server.

Portable school-owned electronic devices will not be left unattended, and instead will be kept out of sight and securely locked when they are not in use.

Portable equipment will be transported in its protective case, if supplied.

Where the school provides mobile technologies, such as phones, laptops and personal digital assistants, for off-site visits and trips, staff will only use these devices.

7. Personal Devices

Staff members will use personal devices in line with the school's Mobile Phone and Smart Devices Use Policy and Code of Conduct for All Adults.

Staff using their own devices will sign an agreement stating that they understand the requirement for routine security checks to take place and the possibility of their personal information being seen by the ICT technician. They will be required to provide consent to their device being accessed – if consent is refused, they will not be permitted to use a personal device.

Approved devices will be secured with a password or biometric access control, e.g. fingerprint scanner.

Multi-factor authentication has been applied to all staff school accounts and staff will need to use this to access school systems on their personal devices.

Members of staff will not contact pupils or parents using their personal devices.

Personal devices will only be used for off-site educational purposes when mutually agreed with the headteacher.

Inappropriate messages will not be sent to any member of the school community.

Permission will be sought from the owner of a device before any image or sound recordings are made on their personal device. Consent will also be obtained from staff, pupils and other visitors if photographs or recordings are to be taken.

Members of staff bringing personal devices into school will ensure that there is not any inappropriate or illegal content on their device.

During lesson times, unless required for the teaching activity being undertaken, personal devices will be kept in a secure location, which cannot be accessed by pupils.

8. Removeable Media

The use of removeable media should be avoided wherever possible. If it is deemed necessary, the media must be encrypted and any data removed as soon as it has been transferred to a secure device.

9. Cloud-Based Storage

School data storage is cloud-based. Data held in remote and cloud-based storage is still required to be protected in line with the UK GDPR and DPA 2018; therefore, members of staff will ensure that cloud-based data is kept confidential and no data is copied, removed or adapted.

10. Storing Messages and Information

Emails and messages stored on school-owned devices will be stored digitally or in a suitable hard copy file and disposed of in accordance with the School's Record Management Policy.

Information and data on the school's network and computers will be kept in an organised manner and should be placed in a location of an appropriate security level.

11. Unauthorised Use

Staff will not be permitted, under any circumstances, to:

- Use the ICT facilities for commercial or financial gain without the explicit written authorisation from the Headteacher.
- Physically damage ICT and communication facilities or school-owned devices.
- Relocate, take off-site, or otherwise interfere with the ICT facilities without the authorisation of the Headteacher. Certain items are asset registered and security marked; their location is recorded by the SBM for accountability. Once items are moved after authorisation, staff will be responsible for notifying the SBM of the new location. The exception to this point is when items are moved to the designated secure room for insurance purposes over holiday periods.
- Use or attempt to use someone else's user account. All users of the ICT facilities will be issued with a unique user account and password. The password will be required to be changed every regularly User account passwords will never be disclosed to or by anyone.
- Use the ICT facilities at any time to access, download, send, receive, view or display any of the following:
    - Any material that is illegal
    - Any message that could constitute bullying, harassment (including on the grounds of sex, race, religion/religious belief, sexual orientation or disability) or any negative comment about other persons or organisations
    - Online gambling
    - Remarks, which may adversely affect the reputation of any organisation or person, whether or not you know them to be true or false
    - Any sexually explicit content, or adult or chat-line phone numbers
- Generate messages or documents that appear to originate from someone else, or otherwise impersonate someone else.
- Install hardware or software without the consent of the Headteacher.
- Introduce any form of stand-alone software or removable hardware likely to cause malfunctioning of the ICT facilities or that will bypass, over-ride or overwrite the security parameters on the network or any of the school's computers.

- Use or attempt to use the school's ICT facilities to undertake any form of piracy, including the infringement of software licenses or other copyright provisions whether knowingly or not. This is illegal.
- Use or attempt to use the school's phone lines for internet or email access unless given authorisation by the headteacher. This will include using or attempting to use any other form of hardware capable of telecommunication, regardless of ownership.
- Use any chat-lines, bulletin boards or pay-to-view sites on the internet. In addition, staff will not download or attempt to download any software of this nature.
- Use the internet for any auctioning activity or to purchase items unless given authority to do so by the headteacher.
- Knowingly distribute or introduce a virus or harmful code onto the school's network or computers. Doing so may result in disciplinary action, including summary dismissal.
- Use the ICT facilities for personal use without the authorisation of the Headteacher. This authorisation will be requested on each occasion of personal use.
- Copy, download or distribute any material from the internet or email that may be illegal to do so. This can include computer software, music, text, and video clips. If a staff member it is not clear that they have permission to do so, or if the permission cannot be obtained, they will not download the material.
- Use, or attempt to use, the communication facilities to call overseas without the authorisation of the Headteacher.
- Obtain and post on the internet, or send via e-mail, any confidential information about other employees, the school, its customers or suppliers.
- Interfere with someone else's use of the ICT facilities.
- Be wasteful of ICT resources, particularly printer ink, toner and paper.
- Use the ICT facilities when it will interfere with their responsibilities to supervise pupils.
- Share any information or data pertaining to other staff or pupils at the school with unauthorised parties. Data will only be shared for relevant processing purposes.
- Operate equipment to record an image beneath a person's clothing with the intention of observing, or enabling another person to observe, the victim's genitals or buttocks without their knowledge or consent, whether exposed or covered by underwear – otherwise known as "upskirting".

Any unauthorised use of email or the internet will likely result in disciplinary action, including summary dismissal, in line with the Disciplinary Policy and Procedure.

If a member of staff is subjected to, or knows about harassment, upskirting or bullying that has occurred via staff email or through the use of school-owned devices, they will report this immediately to the headteacher.

12. Use of School Devices

School equipment, including electronic devices, may be assigned to staff members in order to undertake school-related work.

Equipment and devices will only be assigned to staff members who have read, signed and returned the Acceptable Use Agreement (Appendix A).

Once equipment has been assigned, the receiving staff member will be required to undergo any training required to use the requested equipment, including how to store, handle and undertake any maintenance, e.g. changing batteries.

If the equipment or device is no longer required, staff members will return the equipment to the school as soon as possible, allowing the equipment to be made available to someone else.

Devices will be encrypted and protected to ensure the security of any data they hold.

13. Safety and Security

The school's network is secured using firewalls.

Filtering of websites will ensure that access to websites with known malware are blocked immediately and reported to the Online Safety Lead.

Approved anti-virus software and malware protection will be used on all approved devices.

The school will use mail security technology to detect and block any malware transmitted via email.

Members of staff will ensure that all school-owned electronic devices are made available for any anti-virus updates, malware protection updates and software installations, patches or upgrades, as required.

Programmes and software will not be installed on school-owned electronic devices without permission from the Headteacher.

Staff will not be permitted to remove any software from a school-owned electronic device without permission from the Headteacher.

Members of staff who install or remove software from a school-owned electronic device without seeking authorisation from the Headteacher, may be subject to disciplinary measures.

The use of school devices is secured by requiring personal password log-in by staff.

Passwords will be kept confidential and must not be shared with pupils, unauthorised members of staff or third parties.

Devices will be configured so that they are automatically locked after being left idle for a set time.

Staff members will inform the Headteacher/Online Safety Lead/Business Manager immediately if they believe their account/device my have been subject to any malicious activity. They will stop using the account/device immediately.

14. Loss, theft and damage

For the purpose of this policy, **"damage"** is defined as any fault in a school-owned electronic device caused by the following:

- Connections with other devices, e.g. connecting to printers which are not approved by the ICT technician
- Unreasonable use of force
- Abuse
- Neglect
- Alterations
- Improper installation

Any incident that leads to a school-owned electronic device being lost will be treated in the same way as damage.

The Headteacher will decide whether a device has been damaged due to the actions described above.

The ICT technician will be contacted if a school-owned electronic device has a technical fault.

If a school-owned device is lost or stolen, or is suspected of having been lost or stolen, the ICT technician will be informed as soon as possible to ensure the appropriate steps are taken to disable access to the device and the loss may be reported to the DPO if necessary.

The school will not be responsible for the loss, damage or theft of any personal device, including phones, cameras, tablets, removable media, etc.

15. Implementation

Staff will report any breach of this policy to the headteacher.

Regular monitoring and recording of email messages may be carried out on a random basis. Hard copies of email messages can be used as evidence in disciplinary proceedings.

Use of the telephone system may be logged and monitored.

Use of the school internet connection will be recorded and monitored.

The SBM will conduct random checks of asset registered and security marked items.

The ICT technician may remotely view or interact with any of the computers on the school's network. This may be used randomly to implement this policy and to assist in any difficulties.

The school's network has anti-virus software installed with a centralised administration package; any virus found will be logged to this package.

The school's database systems are computerised. Unless given permission by the ICT technician, members of staff will not access the system. Failure to adhere to this requirement may result in disciplinary action.

All users of the database system will be issued with a unique individual password. Staff will not, under any circumstances, disclose this password to any other person.

Attempting to access the database using another employee's user account and/or password without prior authorisation will likely result in disciplinary action, including summary dismissal.

User accounts will be accessible by the headteacher and the ICT technician.

Users will ensure that critical information is not stored solely within the school's computer system. Hard copies will be kept or stored separately on the system. If necessary, documents will be password protected.

Users will be required to familiarise themselves with the requirements of the UK GDPR and Data Protection Act 2018, and to ensure that they operate in accordance with the requirements of the regulations and the Data Protection Policy.

Any breach of the rules in this policy may result in disciplinary action, which may lead to dismissal.

A misuse or breach of this policy could also result in criminal or civil actions being brought against the persons involved or the school.

Appendix A - Acceptable Use Agreement & Device User Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

For my professional and personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of school ICT systems (e.g. laptops, email, VLE etc) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- Personal mobile devices are not to be used in areas of the school where children are present and must never be connected to the school's wireless internet network.
- I will not use personal email addresses on the school systems.

- I will not connect personal USB devices to school computers.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not access or share materials that support extremist views or actions, or that encourage radicalisation.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless I have consulted the ICT specialist (currently provided by the ICT service).
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Agreement applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Acceptable Use Policy & Agreement

Device User Agreement

- I understand that devices loaned to me remain the property of Fulbourn Primary School and I am able to use them for work related purposes ONLY.
- I understand that devices, whilst in my possession, remain the property of the school.
- I understand that it is my responsibility to ensure the safe-keeping, security and correct use of these items.
- I understand that this equipment may contain confidential information and so it can ONLY be used on the school premises or at home and should only be transported between the school and my home.
- I agree not to use this equipment in any public areas.
- I understand that I will be held responsible for any data loss that may arise as a result of me being found to be in breach of this agreement.
- I agree not to lend any of these items to another person.
- I agree to use this equipment in accordance with the school's Acceptable Use Policy, Acceptable Use Agreement and Code of Conduct.
- I will notify the school immediately of any loss or damage to these items.
- I will return all items to the school upon request of the school, for whatever reason.
- I understand that Imay be help responsible for costs incurred should the items be broken, damaged or lost.
- I agree to return all items to the school immediately upon the termination of my employment/placement at the school and I understand that the school has a right to withhold final payment until the equipment is returned.

By signing this agreement, I acknowledge that I have received the device described above in good working order and I confirm and accept the terms and conditions in relation to its use.

Declaration

I have read and understand the above and agree to use the school ICT systems and devices (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Name		**Job Title**	
Signed		**Date**	