

THE WILLOWS PRIMARY SCHOOL



E-SAFETY POLICY

Author:	ICT Co-ordinator
Date:	September 2026
Review Date:	September 2028
Date approved:	
Signed :	

This policy applies to all members of the school community (including staff, students/pupils, volunteers, governors, parents/carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school.

Both this policy and the Acceptable Use Policies are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, iPads, whiteboards, digital video equipment, etc.) and technologies owned by pupils and staff, but brought onto school premises (such as laptops, mobile phones, smart phones, tablets, smart watches, etc).

The National Curriculum requires pupils to use Information and Communications Technology (ICT) which may include web-based resources and e-mail. The purpose of this document is to outline how this technology will be safely accessed by pupils, staff and visitors of The Willows Primary School, and to identify the measures that are in place to protect all users from access to inappropriate material.

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. ICT is an essential resource to support learning and teaching, and plays an important role in the everyday lives of children, young people and adults.

Schools need to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment and ensure safe and appropriate use of ICT resources. The internet itself is not consistently policed. Therefore, all users need to be aware of the range of risks associated with the use of internet technologies, for example:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to age-inappropriate video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism, copyright infringement and use of Artificial Intelligence
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

The school does everything that could reasonably be expected in order to manage and reduce these risks. Although this policy concerns the use of computing and communications technology, e-safety is not purely a technical issue – it should be managed within the context of child welfare and safeguarding.

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of their children's online experiences.

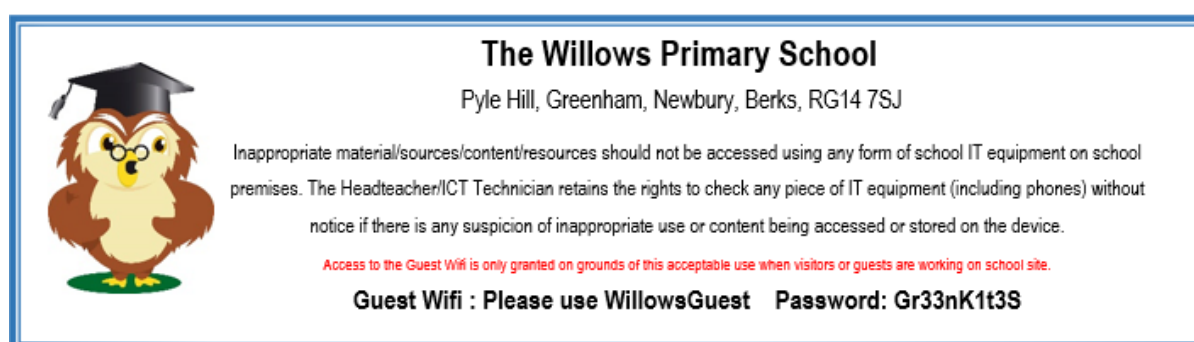
The school helps to educate parents as to the risks of using the internet outside of the school, where children may have more unrestricted use. The school provides information to parents and carers through the school's website and via email, directing them to key websites that provide detailed guidance on e-safety issues.

Internet access is planned to enrich and extend learning activities. Access levels are reviewed to reflect the curriculum requirements and age of pupils. Staff guide pupils in on-line activities that support the learning outcomes planned for the pupils' age and maturity. Pupils are educated in the effective use of the internet in research, including the skills of knowledge location and retrieval.

It is expected that at all times the use of ICT equipment, facilities, and resources will be made by all users in strict compliance with the Acceptable Use Policy which they have signed.

No person will be permitted to use school ICT resources without first agreeing and signing an Acceptable Use Policy appropriate to the intended use.

Access to the Guest Wifi is granted on grounds of acceptable use which is shared and agreed to when Guests sign into the school site.



Pupil use

The pupils have access to a highly filtered internet. Pupils will only use the Internet under close staff supervision with the focus usually on prepared materials. Access will normally be to educational sites that link to areas of the curriculum being delivered at the time. Internet use will therefore be self-limiting and appropriate to the user. Under no circumstances will pupils be allowed access to the Internet without supervision by a staff member. Pupils are taught what is acceptable and what is not acceptable and given clear objectives for internet use. Pupils are not permitted to download programs or files onto school-based technologies or equipment.

Pupils do not have access to social media in school. Pupils will be taught the advantages and pitfalls of social media/networking through our taught e-safety programme.

Teachers will share the **Rules for Responsible Internet Use** (see appendices)

Any breach of the rules for internet use will be referred to the ICT coordinator and the Headteacher. A record will be kept of what has happened, and possibly one or more of the following actions will occur:

- A letter will be sent to parents explaining how the rules have been broken.
- Pupils may be banned from using the Internet and other ICT equipment,
- Any further action decided by the Headteacher.

A planned e-safety programme is provided as part of ICT, PSHE and other lessons and is regularly reviewed to ensure it is up-to-date with respect to new technologies in school and outside school. E-safety sessions are taught in every year group and are a regular focus in both class and whole school assemblies. Additional information on age appropriate use of social

media is regularly shared with parents and advice on restricting and adding parental controls to a variety of mobile devices is shared regularly.

	Y1	Y2	Y3	Y4	Y5	Y6
Media influence:	How do I decide what to do online?	Is everything I see online true?	How do I keep myself safe online?	What is fake news?	Who decides what I experience in the online world?	How do I decide what is true online?
Our online lives:	What should I do if I feel unsafe online?	Who should I talk to online?	How can I be kind and happy online?	How do I decide who to trust online?	How do I thrive online?	What should I share online?

Staff use

- New staff will receive information on the school's Acceptable Use Policy as part of their induction.
- All staff must accept and sign the terms of the Acceptable Use Policy for Staff before using any network or Internet resource in school.
- Staff will be allowed internet use specifically to support their work. Personal use and access to public chat rooms/other kinds of social media will not be allowed on school site or using school IT equipment.
- All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-safety and know what to do in the event of misuse of technology by any member of the school community.
- Staff are not permitted to download programs or files onto school-based technologies without obtaining prior permission from the ICT subject leader or Headteacher.
- Staff may not use personal removable media such as USB memory sticks or portable disk drives on school equipment without first gaining permission from the ICT subject leader or the Headteacher.
- Staff are informed that Internet traffic can be monitored and traced to the individual user. Professional conduct is essential. Staff should report any cases of misuse by children or other staff to the Headteacher. Misuse of the Internet or School Network by staff is a disciplinary matter.

Governor and visitor use

Governors should ensure that they remain conversant with e-safety issues, for example:

- Reading the materials available on the West Berkshire Governors' Services website;
- Attendance at training provided by the Local Authority, National Governors Association, or other relevant organisation;
- Participation in school training and information sessions for staff or parents.

Governors and certain school visitors (e.g. social workers or educational professionals) will be allowed guest access to support their roles. No other access will be allowed. Governors/visitors are not permitted to download programs or files onto school-based technologies without obtaining prior permission from the ICT subject leader or Headteacher.

E-Mail - All users

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced.

E-Mail Pupils - Pupils at The Willows do not use school email addresses.

E-Mail Staff, Governors, Volunteers

- All email communication concerning school business between school staff or governors and any individual or organisation must be conducted using school Microsoft Outlook365 email accounts.
- Under no circumstances should staff or governors conduct any school business using personal e-mail addresses.
- Staff sending e-mails of a particularly sensitive nature, to external organisations or parents, are advised to cc. in the Headteacher. Emails to parents regarding pupils should always go through the school office. Staff should never email pupils.
- Staff must immediately report to the Headteacher the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such e-mail.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Accurate, adequate, relevant and not excessive
- Secure and kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Only transferred to others with adequate protection

Staff must ensure that they:

- Take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse at all times.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.

When personal data is stored on any portable computer system, USB stick or any other removable media:

- The data must be encrypted and password protected.
- The device must be password protected.
- The device must be checked for viruses or malware immediately on connection to school equipment.
- The data must be securely deleted from the device once it has been transferred or its use is complete.

Maintaining the security of information systems

Internet access is managed through RM Unify who provide virus protection and filtering services. The ICT coordinator, HT and IT technician can access, add and amend the blocked sites as and when required. Staff are required to sign an Acceptable Use Policy which outlines the rules for use of the network in order to ensure the safety of both school systems and themselves.

Filtering and Monitoring

Some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material.

Monitoring

The school has monitoring systems in place to protect the school, systems and users:

- The school monitors all network use across all its devices and services.
- Monitoring reports are urgently picked up, acted on and outcomes are recorded by the Designated Safeguarding Lead, all users are aware that the network (and devices) are monitored.
- There are effective protocols in place to report abuse/misuse. There is a clear process for prioritising response to alerts that require rapid safeguarding intervention. (see Responding to incidents of misuse flow chart)
- Management of serious safeguarding alerts is consistent with safeguarding policy and practice.

The school follows the UK Safer Internet Centre [Appropriate Monitoring](#) guidance ([Appropriate Filtering and Monitoring - UK Safer Internet Centre](#)) and protects users and school systems through the use of the appropriate blend of strategies informed by the school's risk assessment.

These may include:

- physical monitoring (adult supervision in the classroom)
- internet use is logged, regularly monitored and reviewed
- filtering logs are regularly analysed (remotely by RM Safety Net) and breaches are reported via the ICT coordinator to senior leaders
- pro-active alerts from RM Safety Net inform the school of breaches to the filtering policy, allowing effective intervention.
- where possible, school technical staff regularly monitor and record the activity of users on the school technical systems
- use of a RM Safety Net assisted monitoring service to review monitoring logs and report issues to school monitoring lead(s)

Filtering

The Willows Primary School's Internet Service Provider (ISP) is operated by BT via RM Unify. This means that the school accesses the Internet through a safe and secure environment. The school has a local server based on site. The email system is provided by Microsoft using the Office365 platform and is hosted in Microsoft data centres.

RM Safety Net is used as the primary filter to ensure inappropriate sites are not reached. Filtering is ongoing but in the unlikely event that material found by users is deemed unsuitable it can be reported to RM to be filtered out. There is also a substantial firewall in place to prevent misuse of the Internet connection which is managed by RM.

The ICT technician ensures that:

- Anti-virus (Trend) is installed on all machines and kept up-to-date;
- school infrastructure and network is as safe and secure as is reasonably possible, and supports third party providers where required to achieve this.
- The school is also responsible for ensuring policies and procedures approved within this policy are implemented. Servers, wireless systems and cabling must be securely located and physical access is restricted.

Teaching pupils to evaluate online content

Pupils are taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. They are taught to acknowledge the source of information and to respect copyright when using online material in their own work. These skills are part of every subject and are taught across the curriculum. If staff or pupils discover unsuitable sites, the URL (address) and content must be reported to the Headteacher or ICT co-ordinator. These sites will be reported to RM SafetyNet, who manage our filtering and will ensure that they are blocked.

Website content

The school has a website which is hosted by Blue Level at www.thewillowsprimary.org. The school website is an essential information resource for parents and others. Items on this site are public. The point of contact on the website is the school address, school e-mail and telephone number. Staff and pupils' work and personal information / e-mail addresses are not published.

The Headteacher takes overall editorial responsibility and ensures that content is accurate and appropriate. The copyright of all material is held by the school or attributed to the owner where permission to reproduce it has been obtained.

Using Digital Photographs, Video, and Sound recordings

- Staff are allowed to take digital photographs, video images, or sound recordings to support educational aims, but must follow school policies concerning the sharing, distribution and publication of such material.
- All parents are asked to complete a photograph consent form authorising the use of such material.
- Images or recordings may only be taken using school equipment; the personal equipment of staff must not be used for such purposes.
- Digital photographs, sound recordings or videos of pupils, staff or work may only be stored on secure GDPR compliant systems. This includes the use of Seesaw as a cloud-based learning journal.
- Visitors wanting to use personal portable media to share images/files (e.g. USB sticks) to deliver presentations, training, etc. must have permission from the Headteacher.
- Visitors will always be encouraged to send presentations/resources in advance of their visit.
- Pupil mobile phones can only be brought onto school, site if approval has been granted by the Headteacher. Any pupils who bring phones onto the school premises have to hand them into main school reception as soon as they arrive and collect them at the end of the day. They are not allowed to use them at all within school.
- Pupils do not use publicly accessible webcams. Webcams in school may only ever be used for specific learning purposes.
- Parents will be reminded at least annually, about the importance of not sharing images of other peoples' children due to child protection reasons, when photos have been allowed at school events.

The use of photos and images of children

We use the guidance developed by the UK Online Harms Early Warning Working Group. This guidance shares best practice and considerations for education settings on the use of photos and videos of children and young people across their websites, online platforms and other digital spaces to address the risk of AI image manipulation.

We ensure that the following image security practices are in place:

- Ensuring images do not contain identifiable information that could be used to harm or blackmail an individual (e.g. full names or faces).
- Using watermarked images and watercolour images wherever possible
- Using imagery that is harder to misuse or abuse, this could be by only sharing photos taken from a distance, blurred images or images taken from over the shoulder.
- Applying privacy settings to help limit who can view and share content
- Removing metadata (e.g. EXIF data) from the images that may reveal location, device details or timestamps.
- Embedding image security awareness and practices in staff training and policies.

Publishing pupils' images and work

The school's website is designed to promote the school and publish resources to support pupils, parents and school life. The safety of information published on the website must be considered from a personal and school security viewpoint.

Photographs that enable pupils to be identified will be selected carefully and only be of those children whose parents have given permission via our Photographic Consent Form. Pupils' full names will not be used anywhere, particularly associated with photographs. Permission to display photographs is obtained as part of the registration process for new pupils with the signing of the Photographic Consent Form

Photographs published on the website, or elsewhere, that include pupils will be selected carefully and will comply with GDPR requirements. Care should be taken not to include images of pupils who for any reason should not be publicly identified i.e. parental consent not received.

Cyberbullying

Cyberbullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, online chat forums and websites. Cyberbullying can be a form of child on child abuse.

Teachers should be aware that, because children have limited access to social media or phones in school, cyberbullying incidents occur most commonly outside of school but that these incidents can have an impact on school life. Further information can be found in our Anti Bullying Policy.

Home Learning

If there is a local lockdown/school closure requiring pupils to remain at home, school has the capacity to offer immediate remote education. Further information on how we ensure that remote/ online learning is as safe as possible can be found in our Remote Learning Policy.

Complaints regarding e-safety

Complaints should be via the office email address and should be addressed to the Headteacher. Complaints concerning Internet access will be handled under the Complaints Policy.

Copyright

The school will ensure that the copying and subsequent use of Internet derived materials by staff and pupils complies with copyright law. All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

Dealing with Incidents

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual. Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or the West Berkshire Council Disciplinary Procedures. Policy breaches may also lead to criminal or civil proceedings.

All incidents would also be logged using one or more of the following school procedures: safeguarding, GDPR or CREST, dependent on the particulars of the incident. For the avoidance of doubt, activities that will cause an e-safety incident to be raised are given below:

Unsuitable, Inappropriate, but legal activities

The following Internet and email activities will not be tolerated on school ICT equipment or services, whether in school or outside. These activities while not illegal are considered by the school as unsuitable or inappropriate. Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Pornography;
- Promotion of any kind of discrimination, racial or religious hatred;
- Threatening behaviour, including promotion of physical violence or mental harm;
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute.

Users may not:

- Run a private business using school ICT equipment, systems, or services;
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by West Berkshire Council or the school;
- Upload, download or transmit commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions;
- Reveal or publicise confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords);
- Create or propagate computer viruses or other harmful files;
- Carry out sustained or instantaneous high volume network traffic (e.g. downloading/uploading files) that causes network congestion and hinders others in their use of the internet;
- Play non-educational on-line games or gamble on-line;
- Use school ICT equipment, systems, or services for Internet file sharing;
- Use social networking sites.

Illegal Activities

The following Internet and email activities are illegal and will not be tolerated on school ICT equipment or services, whether in school or outside.

Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:

- Child sexual abuse images;
- Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation;
- Adult material that potentially breaches the Obscene Publications Act in the UK;
- Criminally racist material in the UK;
- The promotion of terrorism.

The Willows Primary School
Rules for Responsible Internet Use - Pupils

Our school has iPads, netbooks and desktop computers with internet access to help our learning. These rules will help keep us safe.

Using the iPads, netbooks and computers:

- I will not access other people's files;
- I will not bring in portable data sticks or CDs from outside school and try to use them on the school computers.

Using the Internet:

- I will ask permission from a teacher before using the Internet;
- I will report any unpleasant material to my teacher immediately because this will help protect other pupils and myself;
- I understand that the school may check my computer/files and may monitor the internet sites I visit;
- I will not complete and send forms without permission from my teacher;
- I will not give my full name, my home address or telephone number when completing forms.

When using e-mail:

- I will immediately report any unpleasant messages sent to me because this would help protect other pupils and myself;
- I understand that e-mail messages I receive or send may be read by others;
- The messages I send will be polite and responsible;
- I will only e-mail people I know, or my teacher has approved;
- I will only send an e-mail when it has been checked by a teacher;
- I will not give my full name, my home address or telephone number;
- I will not use e-mail to arrange to meet someone outside school hours.

The Willows Primary School
Acceptable Use Policy for ICT (Staff)

Aims

- To allow all users to access and use the Internet/ICT equipment in all forms across the school
- To provide a mechanism by which staff and pupils are protected from sites, information and individuals which would undermine the principles and aims of the school.
- To provide rules which are consistent and in agreement with both GDPR regulations and the Data Protection Act.
- To provide a framework of rules which are consistent with the acceptable procedures commonly used on the internet.
- To ensure accountability for any breach of the rules.

Conditions

1. Personal use of the Internet is only permitted outside 'directed time'.
This is to include, writing personal e-mails and visiting sites such as social networking, selling sites, e-bay/Vinted, holiday companies, insurance companies and ticket agencies.
2. You must not disclose passwords and log-in names to anyone, other than the persons responsible for running and maintaining the system.

Log-in details should remain personal to avoid compromises in security.

3. You must not disclose personal addresses, telephone numbers, school network log-ins or e-mail log-ins of any staff or pupil. *Privacy should be respected at all times.*
4. You must not use names, photographs, video, web cam images or recorded material of pupils without written permission from parents or carers. *This is recorded on the Parental Consent Form.*
5. You must not download, use or upload any material which is copyright. Do not plagiarise other people's work. Permission should be sought from the owner. If in doubt do not use the material.
6. Under no circumstances should you view, upload or download any material which is likely to be unsuitable for children. This applies to any material with violent, dangerous, discriminatory or inappropriate sexual content.
7. Be polite and respect other people's views. The use of strong or inappropriate language or aggressive behaviour is not allowed.
8. The use of chat rooms is forbidden.
9. Illegal activities of any kind are forbidden.
10. Always respect the privacy of files of other users. Do not enter file areas of other staff without their permission.
11. You must log off when you have finished using a computer. There are separate access passwords for pupils and staff to access the computers. Where remote access to the school network is available it is vital to log off and protect log-in details.

This is to avoid unauthorised access to sensitive or shared material and to protect the school network from outside access by unauthorised users.

12. Under **no** circumstances allow pupil access to the Internet without supervision by a staff member. This includes break times, lunchtimes and after school.
13. Ensure that all pupils have followed the correct procedures before, during and after the session, in accordance with the Acceptable Use Policy for Pupils.
14. Report any incident which breaches the Acceptable Use Policy to the Headteacher.
15. In the event of any pupil reporting misuse of e-mail to you, please **DO NOT** delete any offending messages. You must report the details to Headteacher or ICT coordinator who will investigate further and log the incident.
16. Only use portable storage devices when absolutely necessary. Encrypted data sticks, e-mail or transfer between laptop and the school network are the preferred methods.
17. Hall projectors and classroom screens **must** be switched off when not in use. Please refer to the Health & Safety Policy.
18. Mobile telephones must not be used during 'directed time' for personal calls or texts unless in emergency.
19. You must not allow pupils to use a computer (desktop or laptop) while it is logged in as a teacher or adult working in school.
20. Refer to Acceptable Use Policy for School Laptops/IPADS.
21. Refer to Acceptable Use Policy for Pupils.

Declaration:

- I understand and agree to abide by the provisions and conditions of this policy.
- I understand that any breach of the above rules may result in disciplinary action.
- I agree to report any misuse of the system to the Headteacher.

Name (Block Capitals) _____

Signed _____

Date _____

The Willows Primary School

Acceptable Use Policy for School Laptops/iPads

Your school laptop/iPad is on loan to you while you remain employed by The Willows Primary School. While the laptop/iPad is in your care the following points should be noted:

1. The laptop remains the property of The Willows Primary School and is **only** for the use of the member of staff it is issued to. It must be returned to the school in an acceptable condition if the member of staff leaves the school. To this end, the school offers a suitable case for transporting laptops/iPads and this (or another suitable alternative) must be used when transporting devices between home and school.
2. Insurance cover is not provided by the school and staff are reminded that it is their responsibility to provide cover if the laptop is used away from the school premises.
3. Only correctly licensed software/APPs, authorised by the ICT Co-ordinator or IT technician and installed by, or with the permission of the school may be used.
4. Do not remove any programs installed on the laptop on issue.
5. Anti-virus software is installed and **must** be updated by rebooting the laptop while in school. The ICT coordinator can advise/remind staff of this procedure.
6. Any faults with laptops/iPads must be reported to the ICT coordinator as soon as possible. Under no circumstances should staff attempt to repair suspected hardware faults.
7. Training in the use of the laptop/iPad can be provided by the ICT coordinator/ICT Technician.
9. Any charges incurred by staff accessing the internet from home are not chargeable to the school.
10. When the laptop/iPad is returned to school it must be returned to the ICT coordinator. The original laptop/iPad will be re-issued to another member of staff.
11. The laptop/iPad may be recalled for periodic maintenance, with appropriate notice given.
12. The laptop/iPad is issued as a professional tool and is not intended for personal use. It should not be used to store personal items such as photos etc. Inappropriate material/sources/content should not be accessed using any form of school IT equipment – either on or off school premises. The Headteacher/ICT Technician retains the rights to check any piece of IT equipment without notice if there is any suspicion of inappropriate use or content being stored on the device.
13. The iPad should be registered to iCloud using your school email address.

Laptop Make _____

Laptop Model _____

Serial Number _____

Authorised by Headteacher (signature) _____ Date _____

Received by _____

Signed _____ Date _____