Box CE VC Primary School
Online Safety Policy

This policy is based on the 'Wiltshire Schools ICT: Online Safety Policy Template 2012 and the DCFS Cyberbullying – Supporting School Staff, 2009.

This policy should be read in conjunction with other related policies and procedures e.g.

- Child protection policy
- Child protection procedures and record keeping
- Behaviour policy
- Anti-bullying policy
- Intimate care and invasive procedures policy
- Disability and equality scheme
- Whistleblowing policy
- Data Protection Policy
- Computing policy
- Responsible Use of the Internet policy for children
- Acceptable Use of the Internet policy for staff
- Child-Friendly Online safety policy
- Laptop policy for staff
- iPad policy for staff
- Personal Use of Social Media for Staff and Governors policy

Rationale
The internet has become an important aspect of everyday life and children need to be able to use it safely and responsibly. At Box Primary School, we believe that the internet offers a valuable resource for teachers and children, as well as providing new ways to communicate with others worldwide. At the same time our school recognises that there are many risks related to using the internet and this policy sets out the measures to be taken to minimise them.

1. Leadership and Management
The school online safety policy features as part of the policy review cycle and it is related to other policies including those for child protection, behaviour, PSHE and anti-bullying. This policy

Written	This Review	Next Review
May '12	Oct '18	Oct '19

will be reviewed on annual basis by the school's online safety coordinator. It will be ratified by the staff and the governors. Our school's online safety committee (a committee consisting of children, governors and parents) will review the "Responsible Internet Use" section of this policy on a yearly basis. They have also produced a Child Friendly version of our online safety policy, which they review and update yearly. Our online safety procedures are constantly under review. The online safety coordinator, alongside the staff review and update our status using the '360 Safe' online safety review tool as guidance (http://www.360safe.org.uk).

1.2 How will Internet access be authorised?
We believe that internet access for pupils is an entitlement on the basis of educational need and is an essential resource for staff. Parents of reception children complete the Responsible Internet Use agreement form and pupils take responsibility for signing this form from Yr 3. A differentiated form is used with children in KS1, designed for the parents to talk through with their children.

The South West Grid for Learning (SWGfL) proactively monitors internet usage for illegal (attempted access of child abuse and incitement for racial hatred) websites and will notify the local police and Wiltshire Council in these instances.

In school, we will keep a record of all staff and pupils who are granted internet access. The record will be kept up-to-date; for instance if a pupil's access is withdrawn. Children will only use the internet under supervision by adults and at Key Stage 1, access to the internet will be by adult demonstration with directly supervised access to specific, approved online materials.

1.3 How will filtering be managed?
Despite careful design, filtering systems cannot be completely effective due to the speed of change of web content. Levels of access and supervision will vary according to the pupil's age and experience. Internet access is tailored so that it is appropriate for all members of the school community from the youngest pupil to staff.

Teaching staff are given a unique username and password by the online safety coordinator, which gives them filtered internet access. Unfiltered access is available via the 'staff proxy' for special circumstances. To access this, the online safety coordinator can organise limited access. In these exceptional circumstances a record will be kept. This means that teachers can access appropriate filtered content that has educational value, for example, videos on YouTube. This will be regularly reviewed. The online safety coordinator will also review the popular permitted and banned sites accessed by the school.

We work closely in partnership with parents, Wiltshire Council, DFE and the SWGfL to ensure systems to protect pupils are reviewed and improved. If staff or pupils discover unsuitable sites, the URL (web address) and content must be reported to the Internet Service Provider (SWGfL) via the online safety lead (see The Wiltshire E Safety Toolkit for contact details). This should

also be logged by staff into our Internet Incident Log. Website logs will be regularly sampled and monitored. Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable. Any material that we believe to be illegal will be referred to the Internet Watch Foundation.

1.4 How will the risks be assessed?

As the quantity and breadth of the information available through the internet continues to grow it is not possible to guard against every undesirable situation. However, the school will address the issue that it is difficult to remove completely the risk that pupils might access unsuitable materials via the school system.

In common with other media such as magazines, books and video, some material available via the internet is unsuitable for pupils. Box Primary School will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer.

Neither the school nor Wiltshire Council can accept liability for the material accessed, or any consequences of internet access. It is important to remember that the use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990. We will regularly review methods to identify, assess and minimise risks and the head teacher will ensure that the policy is implemented and compliance with the policy is monitored.

Teaching and Learning

2.1 Why is internet use important?

The internet is an essential resource to support teaching and learning. The curriculum requires pupils to learn how to locate, retrieve and exchange information using ICT. In delivering the curriculum, teachers need to plan to integrate the use of communications technology such as web-based resources and e-mail and mobile learning. Computer skills are vital to access life-long learning and employment; indeed computing is now seen as an essential life-skill.

The purpose of internet use in school is to raise educational standards, to promote pupil achievement, well being and to support the professional work of staff and to enhance the school's management information and business administration systems. The internet is an essential part of everyday life for education, business and social interaction. Our school has a duty to provide students with quality internet access as part of their learning experience. It is also important to remember that pupils use the internet widely outside school and need to learn how to evaluate internet information and to take care of their own safety and security.

2.2 How will internet use enhance learning?

Using the internet in education has many benefits including:

- Access to worldwide educational resources including museums and art galleries;
- Inclusion in the National Education Network which connects all UK schools;
- Educational and cultural exchanges between pupils worldwide;
- Vocational, social and leisure use in libraries, clubs and at home;
- Access to experts in many fields for pupils and staff;
- Professional development for staff through access to national developments,
- Educational materials and effective curriculum practice;
- Collaboration across networks of schools, support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Access to learning wherever and whenever convenient.

2.3 How will pupils learn to evaluate internet content?

Information received via the web, e-mail or text message requires good information-handling and digital literacy skills. In particular it may be difficult to determine origin and accuracy, as the contextual clues may be missing or difficult to read. Ideally, inappropriate material would not be visible to pupils using the web but this is not easy to achieve and cannot be guaranteed. In school, we educate pupils about what to do if they experience material that they find distasteful, uncomfortable or threatening.

The teaching of online safety skills is on-going. Each term, the children will also cover an independent lesson, specifically about online safety. We have taken the online safety learning outcomes suggested in the Knowsley Computing scheme of work 2014/15 and the Somerset ELim website and integrated them into our computing subject overview. Teachers then incorporate these skills into their medium term computing plan. Online Safety Day is also celebrated each year throughout the school.

Through Online safety education, pupils will learn:

- To be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- To use age-appropriate tools to research internet content.
- To acknowledge the source of information used and to respect copyright when using internet material in their own work.
- To use social networking responsibly and respectfully.
- How to keep their personal information private and to create secure passwords.
- How to report problems and deal with unwanted communications.

- How to share information safely and responsibly.

3. Communication and Content

3.1 The School Website

The point of contact on the website is the school address, school email and telephone number. Staff or pupils' home information will not be published. Website photographs that include pupils will be selected carefully. Pupils' full names will not be used anywhere on the website. Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Where audio and video are included (e.g. podcasts and video blogging) the nature of the items uploaded will only be included with parental permission. The website complies with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright.

3.2 Managing e-mail

E-mail is an essential means of communication for both staff and pupils. Directed e-mail use can bring significant educational benefits and interesting projects between schools. However, the use of e-mail requires appropriate safety measures. We do not give children personal use of email identities such as john.smith@box.wilts.sch.uk as revealing this information could potentially expose a child to identification by unsuitable people. Pupils should not use personal email addresses in school. However, if a lesson requires the children to use email, it should be strictly monitored by the teacher and using an approved e-mail account on the school system.

Pupils must immediately tell a responsible adult if they receive offensive e-mail. Pupils should use email in an acceptable way. Sending images without consent, messages that cause distress and harassment to others are considered significant breaches of school conduct and will be dealt with accordingly.

All staff will use official school provided email accounts and e-mail sent to an external organisation should be written carefully, in the same way as a letter written on school headed paper. **When sending emails, children should be referred to by their initials. Any sensitive documents sent by email should by password protected. Staff are not allowed to access school e-mail accounts on personal devices. Staff must not send school information to their personal e-mail accounts.**

3.3 On-line communications, social networking and social media

Online communications, social networking and social media services are filtered in school by the SWGfL but are likely to be accessible from home and on mobile devices.

Through regular training, all staff are made aware of the potential risks of using social networking sites or publishing either professionally with students or personally. Staff should be

aware of the importance of considering the material they post, ensuring profiles are secured and how publishing unsuitable material may affect their professional status.

Pupils are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published. We have a key role in teaching young people about the importance of keeping personal information safe.

- Pupils will be taught about how to keep personal information safe when using online services. Examples would include real name, address, mobile or landline phone numbers, school attended, IM and email addresses, full names of friends/family, specific interests and clubs etc.
- Pupils must not reveal personal details of themselves or others in online communication, or arrange to meet anyone.
- Staff wishing to use social media tools with students as part of the curriculum will risk assess the sites before use and check the sites terms and conditions to ensure the site is age appropriate. Staff will obtain documented consent from the senior leadership team before using social media tools in the classroom.
- Staff/class official blogs or wikis are password protected and run with approval from the SLT.
- Personal publishing will be taught via age appropriate sites that are suitable for educational purposes. These are moderated by the school where possible.
- Pupils are advised on security and privacy online and are encouraged to set passwords, deny access to unknown individuals and to block unwanted communications. Pupils are encouraged to approve and invite known friends only on social networking sites and to deny access to others by making profiles private.
- All members of the school community are advised not to publish specific and detailed private thoughts, especially those that may be considered threatening, hurtful or defamatory.
- Concerns regarding students' use of social networking, social media and personal publishing sites (in or out of school) will be raised with their parents/carers, particularly when concerning students' underage use of sites. A record of this will be kept in school.
- Staff personal use of social networking, social media and personal publishing sites will be discussed as part of staff induction and are outlined in our Personal Use of Social Media for Staff and Governors policy.
- In line with, 'Guidance for Safer Working Practice for Adults who Work with Children and Young People' it will not be considered appropriate for staff to engage in personal online communications with children and young people, parents or carers. Express care is also to be taken regarding the use of social networking sites.

For more information regarding social media, please see our Personal Use of Social Media for Staff and Governors policy.

Written	This Review	Next Review
May '12	Oct '18	Oct '19

3.4 Mobile phones and personal devices
Mobile phones and other internet enabled personal devices can be used to communicate in a variety of ways with texting, camera phones and internet accesses all common features.

Children are not allowed to bring mobile devices into school unless the headteacher agrees that it is an 'exceptional circumstance'. In these cases, the class teacher should look after the mobile phone for the child. School staff may confiscate a mobile phone or device if its use has not been sanctioned by the headteacher. Any electronic devices that are brought in to school are the responsibility of the user. Our school accepts no responsibility for the loss, theft or damage of such items.

Staff are not permitted to use their own personal phones or devices for contacting children, young people and their families within or outside of the setting in a professional capacity. Staff must not use personal devices such as mobile phones or cameras to take photos or videos of pupils and will only use work-provided equipment for this purpose. Staff must not use personal devices for any school business including accessing their school e-mail accounts. Personal devices are blocked by our IT security settings from accessing school systems.

Staff should only use their mobile phones or other personal devices in designated breaks. Staff are responsible for their own devices at all times.

3.5 Video Conferencing
Videoconferencing (Skype and MSN) enables users to see and hear each other between different locations. This 'real time' interactive technology has many potential benefits in education.

When doing this, staff must refer to the internet consent agreements prior to children taking part in video conferences. All video conferencing equipment in the classroom must be switched off when not in use and not set to auto answer. Pupils will ask permission from a teacher before making or answering a videoconference call. Video conferencing will be supervised appropriately for the pupils' age and ability.

3.6 Emerging Technologies
Many emerging communications technologies offer the potential to develop new teaching and learning tools, including mobile communications, internet access, collaboration and multimedia tools. Access of new technologies will be denied until they have been deemed appropriate by the SLT. They will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.

3.7 Cyberbullying
Many young people and adults find that using the internet and mobile phones is a positive and creative part of their everyday life. Unfortunately, technologies can also be used negatively. It

is essential that young people, school staff and parents and carers understand how cyberbullying is different from other forms of bullying, how it can affect people and how to respond and combat misuse. Promoting a culture of confident users will support innovation and safety.

Cyberbullying is bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites.

Examples of cyberbullying include nasty text messages or emails, rumours sent by email or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles.

Cyberbullying can be defined as:

'…**'virtual' bullying, which can occur in or outside school. Cyber-bullying is a different form of bullying and can happen at all times of the day, with a potentially bigger audience, and more accessories as people forward on content at a click.'** DfE 2014

DfE and Childnet have produced resources and guidance that can be used to give practical advice and guidance on cyberbullying: http://www.digizen.org/cyberbullying

- Cyberbullying (along with all other forms of bullying) of any member of the school community will not be tolerated. Full details are set out in the school's policies on anti-bullying and behaviour.
- Incidents or allegations of cyberbullying will be investigated following the procedures outlined the anti-bullying policy whether they occur inside or outside school.
- Anyone in our school community who is affected by cyberbullying will be supported in accordance with the anti-bullying policy.
- All incidents of cyberbullying reported to the school will be recorded.
- The school will take steps to identify the bully, where possible and appropriate. This includes examining school system logs, identifying and interviewing possible witnesses, and contacting the service provider and the police, if necessary.
- Pupils, staff and parents/carers are required to work with the school to support the approach to cyberbullying and the school's online safety ethos.

3.8 Data Protection

The quantity and variety of data held on pupils, families and on staff is expanding quickly. While this data can be very useful in improving services, data could be mishandled, stolen or misused. The Data Protection Act 2018 and the General Data Protection Regulations (GDPR) gives individuals the right to know what information is held about them and provides a framework to ensure that personal information is handled properly. It promotes openness in the use of personal information.

All data from which people can be identified is protected. To access the school network, staff must use their unique passwords and usernames on school provided devices. **Staff must password protect sensitive documents when sending them by email**. Children's names will not be referred to directly within the content of emails. All teaching staff are issued with an encrypted pen drive with a password unique to them. These devices are the property of the school and are returned in the event of a staff member leaving. If printing any sensitive information staff will use a secure printing option and ensure that any documents are stored or destroyed in line with Data Protection Act 2018 and GDPR.

All Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018 and GDPR.

More information can be found in the school Data Protection Policy.

3.9 Staff use of Social Media

The school is aware that a great number of adults and children are using social networking sites such as Facebook. According to Ofcom's UK Media Literacy report, "social networking continues to increase and 47% of 10-12 year olds have an active profile" and "over half of internet users say they have a social networking profile (54%) compared to 44% in 2009".

The use of social networking provides us with many benefits, from improved communication skills and a greater understanding of technology to a more open worldview. However, we feel that certain behaviours on such websites can potentially have a detrimental effect on the image of the school, our ability to safeguard our pupils and on the integrity of our staff.

For more information, please see our Personal Use of Social Media for Staff and Governors Policy.

4 Implementation

4.1 Introducing the Policy to Pupils

Many pupils are very familiar with internet use and the culture that surrounds it. As part of our online safety teaching and awareness-raising it is important to discuss the key features with pupils as appropriate for their age. Pupils may need to be reminded of the school rules at the point of internet use.

- All users will sign (or parents their behalf in the case of younger children) a Responsible User Policy.
- The online safety committee will annually update the 'child friendly' version of this policy and present it to the rest of the school.

Written	This Review	Next Review
May '12	Oct '18	Oct '19

- All users will be informed that network and internet use will be monitored.
- An online safety training programme, using the Knowsley Scheme of work and Somerset ELim safety scheme of work is taught across the school.
- Pupil instruction regarding responsible and safe use will precede all internet access.
- Online safety will be included in the PSHE curriculum and will be taught throughout the school as part of computing. Both safe school and home use will be covered.
- Online safety SMART rules and copies of the pupils Responsible Internet Use Policy are posted in all rooms with internet access.
- Safe and responsible use of the internet and technology is reinforced across the curriculum and subject areas.

4.2 Consulting with Staff

It is important that all our staff feel confident to use new technologies in teaching and our school online safety policy will only be effective if all staff subscribe to its values and methods. The staff are involved in the policy review process and are given opportunities to discuss the issues and develop appropriate teaching strategies.

All staff must understand that the rules for information systems misuse for Wiltshire Council employees are specific and that instances resulting in disciplinary procedures and dismissal have occurred. If a member of staff is concerned about any aspect of their ICT or internet use either on or off site, they should discuss this with the computing subject leader to avoid any possible misunderstanding.

- The online safety policy will be formally provided to and discussed with all members of staff. The staff will be involved in its review.
- Staff should be aware that internet traffic is monitored and reported by the SWGfL and can be traced to the individual user. Discretion and professional conduct is essential.
- Up-to-date and appropriate staff training in safe and responsible internet use, both professionally and personally, will be provided for all members of staff.
- All members of staff should be aware that their online conduct out of school could have an impact on their role and reputation within school. Civil, legal or disciplinary action could be taken if they are found to bring the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

4.3 Parents and Online safety

Parents need to be aware of the potential dangers that are associated with online communications, social networking sites and mobile technologies to help ensure their children are not putting themselves at risk.

- The school website is used to promote a number of online safety resource websites that parents can use at home with their children.
- Parents are given the opportunity to take part in regular parent online safety learning sessions. Parents will also be given the opportunity to learn alongside their children in 'parent learning sessions'.
- Through our school newsletter and website, regular information is provided to parents about how to ensure they can work with the school to ensure this resource is used appropriately both within school and home.
- Internet issues will be handled sensitively to inform parents without undue alarm.
- Advice on filtering systems and educational and leisure activities that include responsible use of the internet are available to parents.
- Interested parents will be referred to organisations such as PIN, Parents Online and NCH Action for Children (URLs in reference section).
- All parents are aware of who the computing subject leader is and will receive support information as and when available, e.g. Know It All for Parents.
- The school will carry out an annual online safety survey for parents and children to respond to together. This will help constantly refine the school's approach to online safety education.

4.4. How will complaints be handled?

Parents and teachers must know how and where to report incidents. Prompt action is required if a complaint is made. The facts of the case will need to be established, for instance whether the internet use was within or outside school. A minor transgression of the rules may be dealt with by the teacher as part of normal class discipline. Other situations could potentially be serious and a range of sanctions will be required, linked to our behaviour policy. All record of the incident are kept, e.g. e-mails saved or printed, text messages saved etc. All complaints of a child protection nature will be dealt with in accordance with the LA Child Protection procedures.

- Responsibility for handling incidents will be the responsibility of online safety coordinator and SLT.
- Any complaint about staff misuse must be referred to the headteacher.

Box CE VC Primary School
Acceptable Use Agreement for Staff

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

Written	This Review	Next Review
May '12	Oct '18	Oct '19

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

1. I will use all ICT equipment issued to me in an appropriate way. I will not:
   - Access offensive website or download offensive material.
   - Make excessive personal use of the internet or e-mail.
   - Copy information from the internet that is copyrighted or without the owner's permission.
   - Place inappropriate material onto the internet.
   - Will not send e-mails that are offensive or otherwise inappropriate.
   - Disregard my responsibilities for security and confidentiality.
   - Download files that will adversely affect the security of the laptop and school network.
   - Access the files of others or attempt to alter the computer settings.
   - Update web pages etc. or use pictures or text that can identify the school, without the permission of the headteacher.
   - Attempt to repair or interfere with the components, software or peripherals of any computer that is the property of Box School.

2. I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
3. I will only access the system with my own name and registered password, which I will keep secret.
4. When creating passwords, I will make sure that they are secure, using a mix of numbers, letters, symbols and upper/lower case letters.
5. I will inform the computing subject leader as soon as possible if I know my password is no longer secret.
6. I will always log off the system when I have finished working. ·
7. I understand that the school may, in line with policy, check my computer files and e-mails and may monitor the internet sites I visit.
8. My files should not, routinely, be password protected by my own passwords. Should a confidential matter warrant this, I must gain permission from the headteacher and register the passwords with the headteacher. This applies to sensitive documents sent by email.
9. I will ensure that my data is regularly backed up
10. When sending an email containing potentially sensitive information, I will not use children's full names, but will refer to them by their initials.
11. I will only communicate with students / pupils and parents / carers in accordance with the online safety policy, using official school systems. Any such communication will be professional in tone and manner.
12. If I use removable media, I will ensure that this has been carefully checked to ensure it is free from any type of virus.

Written	This Review	Next Review
May '12	Oct '18	Oct '19

13. If I need to save anything containing potentially sensitive information on removable media, I will do so in accordance with the Online safety policy, using the encrypted memory device provided by Box School.
14. I will always adhere to the Box School Computing, Social Networking and online safety policies.
15. I will not open e-mail attachments unless they come from a recognised and reputable source and if unsure, I will bring it to the attention of the computing subject leader.
16. All joke e-mails and attachments are potentially damaging and undesirable and therefore should not be used.
17. I will report immediately to the headteacher any unpleasant material or messages sent to me.
18. I understand that a criminal offence may be committed by deliberately accessing internet sites that contain certain illegal material.
19. Use for personal financial gain, gambling, political purposes or advertising is forbidden.
20. Storage of e-mails and attachment should be kept to a minimum to avoid unnecessary drain on memory and capacity.
21. Activity that threatens the integrity of the school ICT systems, or activity that attacks or corrupts other systems, is forbidden.

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

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school 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 my network access will be suspended immediately, my laptop removed and that other disciplinary consequences may follow.

Box CE VC Primary School
iPad Policy for School Staff

1. The iPad remains the property of Box Primary School.
2. The iPad is allocated to named member(s) of staff and is their responsibility. If another member of staff borrows it, the responsibility still stays with the teacher allocated. Only Box School staff should use the iPad.
3. On the teacher leaving the school's employment, the iPad is returned to Box School. Staff on extended leave of 4 weeks and over should return their iPads to the school (other than by prior agreement with the headteacher).
4. Whenever possible, the iPad must not be left in an unattended car. If there is a need to do so it should be locked in the boot.
5. The iPad must not be taken abroad, other than as part of a school trip and its use agreed by prior arrangement with the headteacher with evidence of adequate insurance.
6. Users must use protective covers / cases for their iPad.

Written	This Review	Next Review
May '12	Oct '18	Oct '19

7. The iPad screen is made of glass and therefore is subject to cracking and breaking if misused: Never place heavy objects (books, laptops, etc.) on top of the iPad or leave the iPad on the floor.
8. Only a soft cloth or approved laptop screen cleaning solution is to be used to clean the iPad screen.
9. Students can only use the teacher's iPad with permission and close supervision.
10. If any fault occurs with the iPad, it should be referred immediately to the network manager.
11. The iPad would be covered by normal household insurance. If not it should be kept in school and locked up overnight.
12. All material on the iPad must adhere to the policy for responsible e-mail, network and internet use and online safety policy.
13. Users are not allowed to send, access, upload, download or distribute offensive, threatening, pornographic, obscene, or sexually explicit materials.
14. Users are not allowed to have personal music or install apps on their iPad. The technician will be responsible for installing new apps onto the system. Any recommendations for new apps should be made to the headteacher or computing lead.
15. Users must use good judgment when using the camera. The user agrees that the camera will not be used to take inappropriate, illicit or sexually explicit photographs or videos, nor will it be used to embarrass anyone in any way. Any use of camera in toilets or changing rooms, regardless of intent, will be treated as a serious violation.
16. Images of other people may only be made with the permission of those in the photograph.
17. Posting of images / movie on the internet into a public forum is strictly forbidden, without the express permission of the parent of a pupil through the 'Agreement for Parents 2014'
18. Users will set a passcode on their iPad to prevent other Users from misusing it.
19. Jailbreaking is the process of which removes any limitations placed on the iPad by Apple. Jailbreaking results in a less secure device and is strictly prohibited.
20. Individual users are responsible for the setting up and use of any home internet connections and no support will be provided for this by the school.
21. The iPad is subject to routine monitoring by Box Primary School. Devices must be surrendered immediately upon request by the headteacher or designated person.
22. Users in breach of the Responsible Use Policy may be subject to but not limited to; disciplinary action, confiscation, removal of content or referral to external agencies in the event of illegal activity.

Written	This Review	Next Review
May '12	Oct '18	Oct '19