Chaddesley Corbett Endowed Primary School

E-safety Policy

Next review date: June 2019

Last updated: 3rd June 2018

Contents:

Statement of intent

At Chaddesley Corbett, we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for pupils and play an important role in their everyday lives.

Whilst the school recognises the importance of promoting the use of computer technology throughout the curriculum, we also understand the need for safe internet access and appropriate use.

Our school has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all pupils and staff.

The school is committed to providing a safe learning and teaching environment for all pupils and staff, and has implemented important controls to prevent any harmful risks.

Signed by:

	Headteacher	Date:	
	Chair of governors	Date:	

1. Legal framework

1.1. This policy has due regard to all relevant legislation including, but not limited to:

- The General Data Protection Regulation
- Freedom of Information Act 2000

1.2. This policy also has regard to the following statutory guidance:

- DfE (2018) 'Keeping children safe in education'

1.3. This policy will be used in conjunction with the following school policies and procedures:

- Anti-bullying Policy – How we strive to eliminate bullying.
- Safeguarding Policy – Keeping safe online.
- Behaviour Policy – positive strategies for encouraging e-safety and sanctions for disregarding it.

2. Use of the internet

2.1. The school understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

2.2. Internet use is embedded in the statutory curriculum and is therefore an entitlement for all pupils, though there are a number of controls the school is required to implement to minimise harmful risks.

2.3. When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful, including the following:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Exposure to explicit or harmful content, e.g. involving radicalisation
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. Roles and responsibilities

3.1. It is the responsibility of all staff to be alert to possible harm to pupils or staff due to inappropriate internet access or use, both inside and outside of the school, and to deal with incidents of such as a priority.

3.2. The governing board is responsible for ensuring that there are appropriate filtering and monitoring systems in place to safeguard pupils.

3.3. The ICT coordinator, is responsible for ensuring the day-to-day e-safety in the school and managing any issues that may arise.

3.4. The ICT coordinator is responsible for sharing the e-safety policy to SLT, teaching staff, governors, parents, pupils and the wider school community.

3.5. The headteacher is responsible for ensuring that the ICT coordinator and any other relevant staff receive CPD to allow them to fulfil their role and train other members of staff.

3.6. The ICT coordinator will provide all relevant training and advice for members of staff as part of the requirement for staff to undergo regularly updated safeguarding training and be able to teach pupils about online safety.

3.7. The ICT coordinator will regularly monitor the provision of e-safety in the school and will provide feedback to the headteacher.

3.8. The headteacher will establish a procedure for reporting incidents and inappropriate internet use, either by pupils or staff.

3.9. The ICT coordinator will ensure that all members of staff are aware of the procedure when reporting e-safety incidents and will keep a log of all incidents recorded.

3.10. The governing body will evaluate and review this E-safety Policy on a yearly basis, considering the latest developments in ICT and the feedback from staff/pupils.

3.11. The headteacher will review and amend this policy with the ICT coordinator taking into account new legislation, government guidance and previously reported incidents, to improve procedures.

3.12. Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

3.13. All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

3.14. All staff and pupils will ensure they understand and adhere to our Acceptable Use Agreement (Appendix 1), which they must sign and return to the headteacher.

3.15. Parents are responsible for ensuring their child understands how to use computer technology and other digital devices appropriately.

3.16. The headteacher is responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

3.17. All pupils are aware of their responsibilities regarding the use of school-based ICT systems and equipment, including their expected behaviour.

4. E-safety education

Educating pupils:

4.1. An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring that pupils are aware of the safe use of new technology both inside and outside of the school.

4.2. Pupils will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online, including extremist material and the validity of website content.

4.3. Pupils will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.

4.4. Clear guidance on the rules of internet use will be presented in all classrooms.

4.5. Pupils are instructed to report any suspicious use of the internet and digital devices to their classroom teacher.

4.6. PSHE lessons will be used to educate pupils about cyber bullying, including how to report cyber bullying, the social effects of spending too much time online and where to access help.

4.7. The school will hold e-safety events, such as Safer Internet Day and Anti-Bullying Week, to promote online safety.

Educating staff:

4.8. A planned calendar programme of e-safety training opportunities is available to all staff members, including whole school activities and CPD training courses.

4.9. All staff will undergo e-safety training on a termly basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety, as well as current developments in social media and the internet as a whole.

4.10. All staff will undergo regular audits by the ICT coordinator in order to identify areas of training need.

4.11. All staff will employ methods of good practice and act as role models for pupils when using the internet and other digital devices.

4.12. All staff will be educated on which sites are deemed appropriate and inappropriate.

4.13. All staff are reminded of the importance of acknowledging information they access online, in order to avoid copyright infringement and/or plagiarism.

4.14. Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand this E-safety Policy.

4.15. The ICT coordinator will act as the first point of contact for staff requiring e-safety advice.

Educating parents:

4.16. E-safety information will be directly delivered to parents through a variety of formats, including newsletters, the school website and social media.

4.17. Parents' evenings, meetings and other similar occasions will be utilised to inform parents of any e-safety related concerns.

5. E-safety control measures

Internet access:

5.1. Internet access will be authorised once parents and pupils have returned the signed consent form in line with our Acceptable Use Agreement.

5.2. All users in **KS2** and above will be provided with usernames and will be instructed to keep these confidential to avoid any other pupils using their login details.

5.3. Management systems will be in place to allow teachers and members of staff to control workstations and monitor pupils' activity.

5.4. Effective filtering systems will be established to eradicate any potential risks to pupils through access to, or trying to access, certain websites which are harmful or use inappropriate material.

5.5. Filtering systems will be used which are relevant to pupils' age ranges, their frequency of use of ICT systems, and the proportionality of costs compared to risks.

5.6. The ICT coordinator will ensure that use of appropriate filters and monitoring systems does not lead to 'over blocking', such that there are unreasonable restrictions as to what pupils can be taught with regards to online teaching and safeguarding.

5.7. Any requests by staff for websites to be added or removed from the filtering list must be first authorised by the headteacher.

5.8. All school systems will be protected by up-to-date virus software.

5.9. An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

5.10. Master users' passwords will be available to the headteacher for regular monitoring of activity.

5.11. Staff are able to use the internet for personal use during out-of-school hours, as well as break and lunch times.

5.12. Personal use will only be monitored by the ICT coordinator for access to any inappropriate or explicit sites, where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

5.13. Inappropriate internet access by staff may result in the staff member being permitted to use the internet for school purposes only, and prohibited from

using any personal devices. This will be dealt with following the process outlined in the misuse by staff section of this policy.

Email:

5.14. Staff will be given approved email accounts and are only able to use these accounts.

5.15. The use of personal email accounts to send and receive personal data or information is prohibited.

5.16. No sensitive personal data shall be sent to any staff or third parties via email.

5.17. Staff members are aware that their email messages are not monitored.

5.18. Any emails sent by pupils to external organisations will be overseen by their class teacher and must be authorised before sending.

5.19. Chain letters, spam and all other emails from unknown sources will be deleted without opening.

5.20. Staff will not be punished if they are caught out by cyber-attacks as this may prevent similar reports in the future – the ICT coordinator will conduct an investigation; however, this will be to identify the cause of the attack, any compromised data and if there are any steps that can be taken in the future to prevent similar attacks happening.

Social networking:

5.21. Access to social networking sites will be filtered as appropriate.

5.22. Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the headteacher.

5.23. Pupils are regularly educated on the implications of posting personal data online outside of the school.

5.24. Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the school as a whole.

5.25. Staff are not permitted to communicate with pupils over social networking sites and are reminded to alter their privacy settings.

5.26. Staff are not permitted to publish comments about the school which may affect its reputability.

5.27. Staff are not permitted to access social media sites during teaching hours unless it is justified to be beneficial to the material being taught. This will be discussed with the headteacher prior to accessing the social media site.

Published content on the school website:

5.28. The headteacher will be responsible for the overall content of the website and will ensure the content is appropriate and accurate.

5.29. Contact details on the school website will include the phone number, email and address of the school – no personal details of staff or pupils will be published.

5.30. Images and full names of pupils, or any content that may easily identify a pupil, will be selected carefully, and will not be posted until authorisation from parents has been received.

5.31. Pupils are not permitted to take or publish photos of others without permission from the individual.

5.32. Staff are able to take pictures with their school Ipad. Staff will not take pictures using their personal equipment.

5.33. Any member of staff that is representing the school online, e.g. through blogging, must express neutral opinions and not disclose any confidential information regarding the school, or any information that may affect its reputability.

Mobile devices and hand-held computers:

5.34. The headteacher may authorise the use of mobile devices by a pupil where it is seen to be for safety or precautionary use.

5.35. Pupils are not permitted to access the school's Wi-Fi system at any times using their mobile devices and hand-held computers.

5.36. Mobile devices are not permitted to be used during school hours by pupils. Members of staff are allowed to use mobile devices in the staff room and the headteacher/ deputy head's office.

5.37. Staff are permitted to use hand-held computers which have been provided by the school, though internet access will be monitored for any inappropriate use by the ICT coordinator where it is justifiable to be necessary and in doing so, would outweigh the need for privacy.

5.38. The sending of inappropriate messages or images from mobile devices is prohibited.

5.39. Mobile devices will not be used to take images or videos of pupils or staff.

5.40. No mobile device or hand-held computer owned by the school will be used to access public Wi-Fi networks.

5.41. To protect, retrieve and erase personal data, all mobile devices and hand-held computers will be fitted with software to ensure they can be remotely accessed.

5.42. ICT technicians will review all mobile devices and hand-held computers termly to ensure all apps are compliant with data protection regulations, up-to-date and to carry out any required updates.

5.43. ICT technicians will review and authorise any apps and/or computer programmes before they are downloaded – no apps or programmes will be downloaded without express permission from an ICT technician or the ICT coordinator

5.44. Apps will only be downloaded from manufacturer approved stores, e.g. Google Play and the Apple App Store.

Network security:

5.45. Network profiles for each pupil and staff member are created, in which the individual must enter a username and personal password when accessing the ICT systems within the school.

5.46. Staff passwords have a minimum and maximum length, to prevent 'easy' passwords or mistakes when creating passwords.

5.47. Staff passwords will require a mixture of letters, numbers and symbols to ensure they are secure as possible.

5.48. Important folders, e.g. those including pupils' medical records, will be password protected to ensure their security – the ICT coordinator and other designated individual(s) will be the only people who have access to this password. No personal data should be accessible from personal computers and memory sticks.

Virus management:

5.49. Technical security features, such as virus software, are kept up-to-date and managed by the ICT coordinator

5.50. The ICT coordinator will ensure that the filtering of websites and downloads is up-to-date and monitored.

5.51. Firewalls will be switched on at all times – ICT technicians will review these on a weekly basis to ensure they are running correctly and to carryout any required updates.

5.52. Staff members will report all malware and virus attacks to the ICT coordinator immediately.

E-safety committee:

5.53. The E-safety Policy will be monitored and evaluated on a termly basis.

6. Cyber bullying

6.1. For the purpose of this policy, cyber bullying is a form of bullying whereby an individual is the victim of harmful or offensive messages, or the posting of information or images online.

6.2. The school recognises that both staff and pupils may experience cyber bullying and will commit to preventing any instances that should occur.

6.3. The school will regularly educate staff, pupils and parents on the importance of staying safe online, as well as being considerate to what they post online.

6.4. Pupils will be educated about online safety through teaching and learning opportunities as part of a broad and balanced curriculum; this includes covering relevant issues within PSHE lessons as well as sex and relationship education.

6.5. The school will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and pupils.

6.6. The school has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.

6.7. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a pupil.

7. Reporting misuse

7.1. Chaddesley Corbett will clearly define what is classed as inappropriate behaviour in the Acceptable Use Agreement, ensuring all pupils and staff members are aware of what behaviour is expected of them.

7.2. Inappropriate activities are discussed and the reasoning behind prohibiting activities due to e-safety are explained to pupils as part of the curriculum in order to promote responsible internet use.

Misuse by pupils:

7.3. Teachers have the power to discipline pupils who engage in misbehaviour with regards to internet use.

7.4. Any instances of misuse should be immediately reported to a member of staff, who will then report this to the headteacher, using a complaints form.

7.5. Any pupil who does not adhere to the rules outlined in our Acceptable Use Agreement and is found to be wilfully misusing the internet, will have a letter sent to their parents explaining the reason for suspending their internet use.

7.6. Members of staff may decide to issue other forms of disciplinary action to a pupil upon the misuse of the internet. This will be discussed with the headteacher and will be issued once the pupil is on the school premises.

7.7. Complaints of a child protection nature, such as when a pupil is found to be accessing extremist material, shall be dealt with in accordance with our Safeguarding Policy.

Misuse by staff:

7.8. Any misuse of the internet by a member of staff should be immediately reported to the headteacher, using a complaints form.

7.9. The headteacher will deal with such incidents and may decide to take disciplinary action against the member of staff.

7.10. The headteacher will decide whether it is appropriate to notify the police or anti-social behaviour coordinator in their LA of the action taken against a member of staff.

7.11.

Pupil sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Refer to:					Inform:	Action:		
	Class teacher	E-safety coordinator	Refer to head teacher	Refer to Police	Refer to e-safety coordinator for action re filtering / security etc	Parents / carers	Remove of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔	✔	✔	✔	✔	✔
Unauthorised use of non-educational sites during lessons	✔				✔				
Unauthorised use of mobile phone / digital camera / other handheld device	✔					✔	✔		
Unauthorised use of social networking / instant messaging / personal email	✔	✔			✔	✔		✔	
Unauthorised downloading or uploading of files	✔						✔	✔	
Allowing others to access school network by sharing username and passwords	✔	✔	✔		✔		✔	✔	
Attempting to access the school network, using another pupil's account	✔				✔		✔		
Attempting to access or accessing the school network, using the account of a member of staff	✔		✔		✔	✔		✔	
Corrupting or destroying the data of other users	✔		✔		✔	✔	✔	✔	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔	✔	✔		✔	✔	✔	✔	
Continued infringements of the above, following previous warnings or sanctions	✔	✔	✔			✔	✔		✔
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	✔		✔					✔	
Using proxy sites or other means to subvert the school's filtering system	✔	✔	✔		✔	✔	✔	✔	
Accidentally accessing offensive or pornographic material and failing to report the incident	✔	✔			✔	✔			
Deliberately accessing or trying to access offensive or pornographic material	✔	✔	✔		✔	✔	✔		✔
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	✔		✔		✔		✔		

Staff sanctions

The indication of possible sanctions in this table should not be regarded as absolute. They should be applied according to the context of any incident and in the light of consequences resulting from the offence.

	Refer to:						
	Head teacher	Local Authority / HR	Police	Technical Support Staff for action re filtering etc	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	✔	✔	✔	✔		✔	✔
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	✔				✔		
Unauthorised downloading or uploading of files				✔	✔		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	✔			✔	✔	✔	
Careless use of personal data e.g. holding or transferring data in an insecure manner	✔	✔		✔	✔		✔
Deliberate actions to breach data protection or network security rules	✔	✔		✔	✔	✔	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✔	✔				✔	✔
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✔				✔	✔	
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	✔			✔			
Actions which could compromise the staff member's professional standing	✔						
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school					✔		
Using proxy sites or other means to subvert the school's filtering system				✔	✔		✔
Accidentally accessing offensive or pornographic material and failing to report the incident	✔			✔	✔		
Deliberately accessing or trying to access offensive or pornographic material	✔	✔		✔	✔	✔	✔
Breaching copyright or licensing regulations					✔		
Continued infringements of the above, following previous warnings or sanctions	✔			✔			✔

Use of illegal material:

7.12. In the event that illegal material is found on the school's network, or evidence suggest that illegal material has been accessed, the police will be contacted.

7.13. Incidents will be immediately reported to the Internet Watch Foundation and the police will be contacted if the illegal material is, or is suspected to be, a child sexual abuse image hosted anywhere in the world, a non-photographic child sexual abuse image hosted in the UK, or criminally obscene adult content hosted in the UK.

7.14. If a child protection incident is suspected, the school's child protection procedure will be followed – the DSL and headteacher will be informed and the police contacted.

8. Monitoring and review

8.1. The ICT coordinator will evaluate and review this E-safety Policy on a yearly basis, taking into account the school's e-safety calendar, the latest developments in ICT and the feedback from staff/pupils.

8.2. This policy will also be reviewed on an annual basis by the governing body; any changes made to this policy will be communicated to all members of staff.

8.3. Members of staff are required to familiarise themselves with this policy as part of their induction programmes.

9. Appendix 1 – Acceptable Use Agreement templates

1.1 Appendix 1a – Acceptable use policy agreement – pupil (KS1)

This is how we stay safe when we use computers:

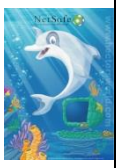
- I will ask an adult if I want to use the internet
- I will only use activities if an adult says it is OK.
- I will take care of the computer and other equipment
- I will ask for help from an adult if I am not sure what to do or if I think I have done something wrong.
- I will close the screen and tell an adult if I see something that upsets me on the screen.
- I know that if I break the rules I might not be allowed to use a computer.

I understand these computer rules and will do my best to keep them

My name:	
Signed (child):	
OR Parent's signature:	
Date:	

Key Stage 1

At Chaddesley Corbett School we think then click



These rules help us to stay safe on the Internet

We only use the internet when an adult is with us

We can click on the buttons or links when we know what they do.

We can search the Internet with an adult.

We always ask if we get lost on the Internet.

We can send and open emails with our teacher.

We can write polite and friendly emails to people that we know, with our teacher.

1.2 Appendix 1b – Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Chaddesely Corbett School I must use technology in a responsible way.

For my own personal safety:

- I understand that my use of technology (especially when I use the internet) will be supervised and monitored.
- I will keep my password safe and will not use anyone else's (even with their permission)
- I will keep my own personal information safe as well as that of others.
- I will turn off or hide the screen and tell a trusted adult if anything makes me feel uncomfortable or upset when I see it online.

For the safety of others:

- I will not interfere with the way that others use their technology.
- I will be polite and responsible when I communicate with others,
- I will not take or share images of anyone without their permission.

For the safety of the school:

- I will not try to access anything illegal.
- I will not download anything that I do not have the right to use.
- I will not use my own personal device
- I will not deliberately bypass any systems designed to keep the school safe.
- I will tell a responsible person if I find any damage or faults with technology, however this may have happened.
- I will not attempt to install programmes of any type on the devices belonging to the school without permission.
- I will only use social networking, games sites and chat through the sites the school allows

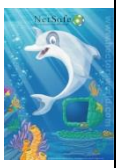
KS2 Pupil Acceptable Use Agreement Form

I understand that I am responsible for my actions and the consequences. I have read and understood the above and agree to follow these guidelines:

Name:	
Signed:	
Date:	

Key Stage 2

At Chaddesley Corbett School we think then click



e-Safety Rules for Key Stage 2

- **We ask permission before using the Internet.**
- **We only use websites that an adult has chosen.**
- **We tell an adult if we see anything we are uncomfortable with.**
- **We immediately 'hide' any webpage we not sure about, and tell a teacher.**
- **We only e-mail people when a teacher has given permission.**
- **We send e-mails that are polite and friendly.**
- **We never give out personal information or passwords.**
- **We never arrange to meet anyone we don't know.**
- **We do not open e-mails sent by anyone we don't know.**
- **We do not use Internet chat rooms.**

1.3 Appendix 1c - Acceptable Use Agreement – staff & volunteer

Background

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

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 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, learning platform) 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 in the e-safety policy.
- 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 will immediately report any illegal, inappropriate or harmful material or incident of which I become aware, 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 images. I will not use my personal equipment to record these images.
- Where images are published (e.g. on the school website / learning platform) I will ensure that it will not be possible to identify by name, or other personal information, those who are featured. (see section A.3.3 of the e-safety policy)
- I will only use chat and social networking sites in school in accordance with the school's policies. (see section A.3.2 of the e-safety policy)
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (see sections A.3.1 and A.3.2 of the e-safety policy)
- 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:

- I will only use my personal mobile ICT devices as agreed in the e-safety policy (see section A.3.1) and then with the same care as if I was using school equipment. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will avoid using a personal email address on the school ICT systems whenever possible. (A.3.2).
- I will not open any attachments to emails, unless the source is known and trusted, 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 (see **IBS Schools Systems and Data Security advice**).

- 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 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 this is allowed in school policies.
- 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 LA Personal Data Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I will not take or access pupil data, or other sensitive school data, off-site without specific approval. If approved to do so, I will take every precaution to ensure the security of the data,
- 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 school 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 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 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 out of school and to my use of personal equipment in school or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could involve a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police (see section A.2.6).

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines.

Staff / volunteer Name:	
Signed:	
Date:	

1.4 Appendix 1d - Acceptable use policy agreement and permission forms – parent / carer

Technology has transformed learning, entertainment and communication for individuals and for all organisations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure that:

- young people stay safe and will be responsible users and stay safe while using ICT (especially the internet).
- school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

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

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Child's name	
Parent's name	
Parent's signature:	
Date:	

Permission for my child to use the internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe and responsible use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use Agreement.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the school if I have concerns over my child's e-safety.

Parent's signature:	
Date:	

Permission to publish my child's work (including on the internet)

It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet, via the school website.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

Permission to for my child to participate in video-conferencing

Videoconferencing technology is used by the school in a range of ways to enhance learning – for example, by linking to an external "expert", or to an overseas partner school. Video conferencing only takes place under teacher-supervision. Independent pupil use of video-conferencing is not allowed.

As the parent / carer of the above child I give my permission for this activity.

Parent's signature:	
Date:	

The school's e-safety Policy, which contains this Acceptable Use Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Appendix 1e - Acceptable use policy agreement – community user

You have asked to make use of our school's ICT facilities. Before we can give you a log-in to our system we need you to formally agree to use the equipment and infrastructure responsibly.

For my professional and/or personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- 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 will immediately report any illegal, inappropriate or harmful material or incident, of which I become aware, to a member of the school's staff.

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

- I will not access, copy, remove or otherwise alter any other user's files or data, 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.

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:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 described above.
- 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, except with the specific approval of the school.

- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

I have read and understand the above and agree to use the school ICT systems (both in and out of school) within these guidelines. I understand that failure to comply with this agreement will result in my access to the school's ICT systems being withdrawn, that further actions will be taken in the event illegal activity, and that I may be held liable for any damage, loss or cost to the school as a direct result of my actions.

Community user Name:	
Signed:	
Date:	

10. Appendix 2 - Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behaviour and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc.

Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

- Have more than one senior member of staff / volunteer involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. *This will automatically be done for you if you are using Policy Central from Forensic Software or other monitoring software.* It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

    - Internal response or discipline procedures
    - Involvement by Local Authority or national / local organisation (as relevant).
    - Police involvement and/or action
- If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
    - incidents of 'grooming' behaviour
    - the sending of obscene materials to a child
    - Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.
- It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Sample documents for recording the review of and action arriving from the review of potentially harmful websites can be found in the PDF version of the SWGfL template e-safety policy (pages 36-38): http://www.swgfl.org.uk/Files/Documents/esp_template_pdf

11. Appendix 3 – Criteria for website filtering

A. ORIGIN - What is the website's origin?

- The organisation providing the site is clearly indicated.
- There is information about the site's authors ("about us", "our objectives", etc.)
- There are contact details for further information and questions concerning the site's information and content.
- The site contains appropriate endorsements by external bodies and/or links to/from well-trusted sources

B. CONTENT - Is the website's content meaningful in terms of its educational value?

- The content is age-appropriate
- The content is broadly balanced in nature, and does not appear unduly biased, partisan or unreliable
- The site is free of spelling mistakes, grammatical errors, syntax errors, or typos.
- **The site promotes equal and just representations of racial, gender, and religious issues.**
- **The site does not contain inappropriate content such as pornography, abuse, racial hatred and terrorism.**
- **The site does not link to other sites which may be harmful / unsuitable for the pupils**
- The content of the website is current.

C. DESIGN - Is the website well designed? Is it / does it:

- appealing to its intended audience (colours, graphics, layout)?
- easy to navigate through the site - links are clearly marked etc?
- have working links?
- have inappropriate adverts?

D. ACCESSIBILITY - Is the website accessible?

- Does it load quickly?
- Does the site require registration or passwords to access it?
- Is the site free from subscription charges or usage fees?

12. Appendix 4 - Supporting resources and links

The following links may help those who are developing or reviewing a school e-safety policy.

General

South West Grid for Learning "SWGfL Safe" - http://www.swgfl.org.uk/Staying-Safe

Child Exploitation and Online Protection Centre (CEOP) http://www.ceop.gov.uk/

ThinkUKnow http://www.thinkuknow.co.uk/

ChildNet http://www.childnet-int.org/

InSafe http://www.saferinternet.org/ww/en/pub/insafe/index.htm

Byron Reviews ("Safer Children in a Digital World") - http://www.education.gov.uk/ukccis/about/a0076277/the-byron-reviews

Becta – various useful resources now archived http://webarchive.nationalarchives.gov.uk/20101102103654/http:/www.becta.org.uk

London Grid for Learning - http://www.lgfl.net/esafety/Pages/education.aspx?click-source=nav-esafety

Kent NGfL http://www.kented.org.uk/ngfl/ict/safety.htm

Northern Grid - http://www.northerngrid.org/index.php/resources/e-safety

National Education Network NEN E-Safety Audit Tool - http://www.nen.gov.uk/hot_topic/13/nen-e-safety-audit-tool.html

WMNet – http://www.wmnet.org.uk

WES Worcestershire E-Safety Site – http://www.wes.networcs.net

EU kids Online http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/Home.aspx

Cyber Bullying

Teachernet "Safe to Learn – embedding anti-bullying work in schools" (Archived resources)

http://tna.europarchive.org/20080108001302/http://www.teachernet.gov.uk/wholeschool/behaviour/tacklingbullying/cyberbullying/

Anti-Bullying Network - http://www.antibullying.net/cyberbullying1.htm

Cyberbullying.org - http://www.cyberbullying.org/

East Sussex Council - Cyberbullying - A Guide for Schools:

https://czone.eastsussex.gov.uk/supportingchildren/healthwelfare/bullying/Pages/eastsussexandnationalguidance.aspx

CyberMentors: young people helping and supporting each other online - http://www.cybermentors.org.uk/

Social networking

Digizen – "Young People and Social Networking Services": http://www.digizen.org.uk/socialnetworking/

Ofcom Report: Engaging with Social Networking sites (Executive Summary)

http://www.ofcom.org.uk/advice/media_literacy/medlitpub/medlitpubrss/socialnetworking/summary/

Connect Safely - Smart socialising: http://www.blogsafety.com

Mobile technologies

"How mobile phones help learning in secondary schools":

http://archive.teachfind.com/becta/research.becta.org.uk/upload-dir/downloads/page_documents/research/lsri_report.pdf

"Guidelines on misuse of camera and video phones in schools"
http://www.dundeecity.gov.uk/dundeecity/uploaded_publications/publication_1201.pdf

Data protection and information handling

Information Commissioners Office - Data Protection:

http://www.ico.gov.uk/Home/what_we_cover/data_protection.aspx

See also Becta (archived) resources above

Parents' guide to new technologies and social networking

http://www.iab.ie/

1.4.1

Links to other resource providers

SWGfL has produced a wide range of information leaflets and teaching resources, including films and video clips – for parents and school staff. A comprehensive list of these resources (and those available from other organisations) is available on the "SWGfL Safe" website: http://www.swgfl.org.uk/staying-safe

BBC Webwise: http://www.bbc.co.uk/webwise/

Kidsmart: http://www.kidsmart.org.uk/default.aspx

Know It All - http://www.childnet-int.org/kia/

Cybersmart - http://www.cybersmartcurriculum.org/home/

NCH - http://www.stoptextbully.com/

Chatdanger - http://www.chatdanger.com/

Internet Watch Foundation: http://www.iwf.org.uk/media/literature.htm

Digizen – cyber-bullying films: http://www.digizen.org/cyberbullying/film.aspx

London Grid for Learning: http://www.lgfl.net/esafety/Pages/safeguarding.aspx?click-source=nav-toplevel

13. Appendix 5 - Glossary of terms

AUA	Acceptable Use Agreement – see templates earlier in this document
Becta	British Educational Communications and Technology Agency (former government agency which promoted the use of information and communications technology – materials and resources are archived and still relevant)
CEOP	Child Exploitation and Online Protection Centre (part of UK Police), dedicated to protecting children from sexual abuse. Providers of the Think U Know programmes.
DfE	Department for Education
FOSI	Family Online Safety Institute
ICT	Information and Communications Technology
ICT Mark	Quality standard for schools provided by NAACE for DfE
INSET	In-service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
IWF	Internet Watch Foundation
JANET	Provides the broadband backbone structure for Higher Education and for the National Education Network and Regional Broadband Consortia
KS1; KS2	KS1 = years 1 and 2 (ages 5 to 7) KS2 = years 3 to 6 (age 7 to 11)
LA	Local Authority
LAN	Local Area Network
Learning platform	An online system designed to support teaching and learning in an educational setting
LSCB	Local Safeguarding Children Board
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (eg WMNet) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)

Ofsted	Office for Standards in Education, Children's Services and Skills
PDA	Personal Digital Assistant (handheld device)
PHSE	Personal, Health and Social Education
SRF	Self Review Framework – a tool maintained by Naace used by schools to evaluate the quality of their ICT provision and judge their readiness for submission for the ICTMark
SWGfL	South West Grid for Learning – the Regional Broadband Consortium of SW Local Authorities and recognised authority on all matters relating to e-safety (on whose policy this one is based)
URL	Universal Resource Locator – a web address
WMNet	The Regional Broadband Consortium of West Midland Local Authorities – provides support for all schools in the region and connects them all to the National Education Network (Internet)
WSCB	Worcestershire Safeguarding Children Board (the local safeguarding board)