Frenchay C. of E. Primary School

Equality Impact Assessment (EIA)Part 1: EIA Screening

Policies, Procedures or Practices:	e-safety	**DATE:**	May 2019
EIA CARRIED OUT BY:	Katherine Marks	**EIA APPROVED BY:**	Governors

Groups that may be affected:

Are there concerns that the policy could have a different impact on any of the following groups? (please tick the relevant boxes)	Existing or potential adverse impact	Existing or potential for a positive impact
Age (young people, the elderly; issues surrounding protection and welfare, recruitment, training, pay, promotion)		
Disability (physical and mental disability, learning difficulties; issues surrounding access to buildings, curriculum and communication)		
Gender reassignment (transsexual)		
Marriage and civil partnership		
Pregnancy and maternity		
Racial groups (consider: language, culture, ethnicity including gypsy/traveller groups and asylum seekers)		
Religion or belief (practices of worship, religious or cultural observance, including non-belief)		
Sex (male, female)		
Sexual orientation (gay, lesbian, bisexual; actual or perceived)		

Any adverse impacts are explored in a Full Impact Assessment

FRENCHAY C OF E PRIMARY SCHOOL

E-safety Policy

Rationale

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.

The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and learners learn from each other. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and young people should have an entitlement to safe internet access at all times.

The requirement to ensure that children and young people are able to use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in schools are bound. This school e-safety policy should help to ensure safe and appropriate use.

The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote pupil / student achievement.

However, the use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may face include:

- *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, including*

the sending and receiving of inappropriate text, picture or video messages ('sexting')

- *Inappropriate communication / contact with others, including strangers*
- *Inappropriate use of social media, including under age use and contacting staff members*
- *Cyber-bullying*
- *Access to unsuitable video / internet games*
- *An inability to evaluate the quality, accuracy and relevance of information on the internet*
- *Plagiarism and copyright infringement*
- *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.*

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' / pupils' resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

Scope of policy

This policy applies to all members of the school community (including staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of school ICT systems, both in school and out of school where actions relate directly to school set activity or use of school online systems. The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents such as cyber-bullying, which may take place out of school, but are linked to membership of the school. The school will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, inform parents / carers of known incidents of inappropriate e-safety behaviour that take place out of school.

The following sections outline the roles and responsibilities, policy statements and education in relation to e-safety for individuals and groups within the school.

Roles and Responsibilities

These are clearly detailed in Appendix 1 for all members of the school community.

The Head teacher is responsible for ensuring the safety (including e-safety) of members of the school community, though the day to day responsibility for e-safety is delegated to the E-Safety Leader.
The designated person for child protection is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from sharing of personal data, access to illegal / inappropriate materials, inappropriate on-line contact with adults / strangers, potential or actual incidents of grooming and cyber-bullying.

Induction processes

- All new staff receive online-safety training as part of their induction programme.
- Parents of new reception children will receive a briefing about online safety and processes when their child starts school. There are also updates to this throughout the key stages.
- Parents of children who join school mid-year are made aware of the processes and their children are also introduced to the acceptable use policy.
- Parents will be asked to sign a letter confirming that their children have been shown and have agreed to the acceptable use policy.

Staff

There is a planned programme of e-safety training for all staff to ensure they understand their responsibilities, as outlined in this, and the acceptable use policies.

- All new staff receive e-safety training as part of their induction programme.
- All staff will adhere to the acceptable use agreement.
- The E-Safety Leader receives regular updates through attendance at SWGfL and LA training sessions and by reviewing regular e-safety updates from the local authority.
- This E-Safety policy and its updates shared and discussed in staff meetings.
- The E-Safety Leader provides advice/guidance and training as required to individuals as required and seeks LA advice on issues where required.

Governors

Governors should take part in e-safety training / awareness sessions, with particular importance for those who are members of any subcommittee / group involved in ICT / e-safety / health and safety / child protection. This may be offered in a number of ways:

- *Attendance at training provided by the Local Authority / National Governors Association / SWGfL or other relevant organisation.*
- *Information sessions for staff or parents (in school or in other establishments)*

Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating learners to take a responsible approach. The education of students in e-safety is therefore an essential part of our school's e-safety provision. Children and young people need the help and support of the school to recognise and avoid e-safety risks and build their resilience.

- There is a planned e-safety programme (scheme of work) detailed below.
- Key e-safety messages are reinforced annually through lessons, assemblies etc.
- Students are helped to understand the student acceptable use policy and act accordingly
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils sign an acceptable use agreement (See Appendix 2) and this is also communicated to parents who we hope will reinforce the messages at home.
- Pupils are helped to understand the student acceptable use policy and school rules for online safety and encouraged to act accordingly
- Rules for use of ICT systems are posted in all rooms where ICT is used and displayed on log-on screens.
- Staff act as good role models in their own use of ICT.

Curriculum

E-safety is a focus in all relevant areas of the curriculum. The e-safety scheme of work is linked to the National Curriculum key areas of safety and is approved by the LA as part of the Computing scheme of work. It identifies for each year group progression statements, learning outcomes, processes, skills and techniques, vocabulary, suggested software and web links, sample activities and assessment activities. Staff are encouraged to use the resources and information from https://www.thinkuknow.co.uk/ for the teaching of e-safety, in conjunction with the South Glos scheme of work.

- In lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use and processes are in place for dealing with any unsuitable material that is found in internet searches. Staff pre check any searches.
- Where students are allowed to freely search the internet, e.g. using search engines, staff are vigilant in monitoring the content of the websites the young people visit and encourage students to use specific search terms to reduce the likelihood of coming across unsuitable material. It may be appropriate to use a child specific search engine, although this is not always practicable.
- Students are taught to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.

Parents / Carers

Parents and carers may have only a limited understanding of e-safety issues and may be unaware of risks and what to do about them. They have a critical role to play in educating

and supporting their children with managing e-safety risks at home, reinforcing key messages about e-safety and regulating their home experiences. The school supports parents to do this by:

- Providing clear acceptable use policy guidance and regular newsletter and web site updates
- Providing an awareness raising meeting for parents
- Inviting parents to attend activities such as e-safety assemblies and parent's evenings.
- Curriculum activities
- If online safety issues occur, parents are notified by email with appropriate advice.
- Events such as Safer Internet Day
- Providing information and weblinks about where to access support and guidance are on our website.

Parents of children new to the school are provided with an overview of expectations linked to relevant policies including online safety when their child starts school.

Technical Staff - Roles and Responsibilities

For **all** schools, the local authority provides technical guidance for e-safety issues, and the team are fully informed about the issues. Downend Secondary school provide technical support to the school and the "administrator" passwords for the school are not held by the school. Downend are responsible for their security and any implications of their use.

The school ensures, when working with our technical support provider, that the following guidelines are adhered to.

School ICT systems will be managed in ways that ensure that the school meets the e-safety technical requirements outlined in the SWGfL Security Policy and Acceptable Usage Policy and any relevant Local Authority E-Safety Policy and guidance

- There will be regular reviews and audits of the safety and security of school ICT systems as directed

  by LA and technical advice.

- All users will have clearly defined access rights to school ICT systems. Details of the access rights available to groups of users will be reviewed by the Network Manager

- All users will be provided with a username and password (if appropriate).
- The "master / administrator" passwords for the school ICT system, used by the Network Manager (or other person) must also be available to the Head teacher or other nominated senior leader.
- Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- The school maintains and supports the managed filtering service provided by an external LA approved agency.
- Any filtering issues should be reported immediately to the ICT leader or Head teacher, who will contact the LA or filtering system agency as appropriate.
- The school infrastructure and individual workstations are protected by up to date virus software.
- School ICT technical staff regularly monitor and record the activity of users on the school ICT systems and users are made aware of this in the Acceptable Use Policy.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, hand held devices etc from accidental or malicious attempts which might threaten the security of the school systems and data.

- An agreed policy is in place for the provision of temporary access of "guests" (eg trainee teachers, visitors) onto the school system.

Use of digital and video images - Photographic, Video

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff and students / pupils need to be aware of the risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. This is especially true of 'sexting', where inappropriate messages or images may be sent between two mobile phones. There are reported incidents of employers carrying out internet searches for information about potential and existing employees. The school informs and educates users about these risks and implements policies to reduce the likelihood of the potential for harm:

- When using digital images, staff educate students / pupils about the risks associated with the taking, use, sharing, publication and distribution of images including on social networking sites.
- Staff are allowed to take digital / video images to support educational aims, but follow guidance in the acceptable use policy concerning the sharing, distribution and publication of those images. Staff must use cameras which are for school use only. They must never use their mobile phones to take photographs in school or on school trips.
- With the exception of school trips or visits, staff should not remove digital devices from the school which have images of children stored on them.
- The headteacher has a role to play in encouraging parents and carers not to take photographs of children other than their own during school activities (for example sports' day and school trips when they are volunteering).
- It is the role of the headteacher and / or computing subject leader to educate parents and carers in the safe sharing of images on social media, and to ensure steps are taken to remove images of children from these sites which may place vulnerable children at risk of harm.
- Staff ensure that pupils also act in accordance with their acceptable use policy.
- Student's work is only published on a public web site with the permission of the student and parents or carers.

Guidance on the Use of Communications Technologies

A wide range of communications technologies have the potential to enhance learning

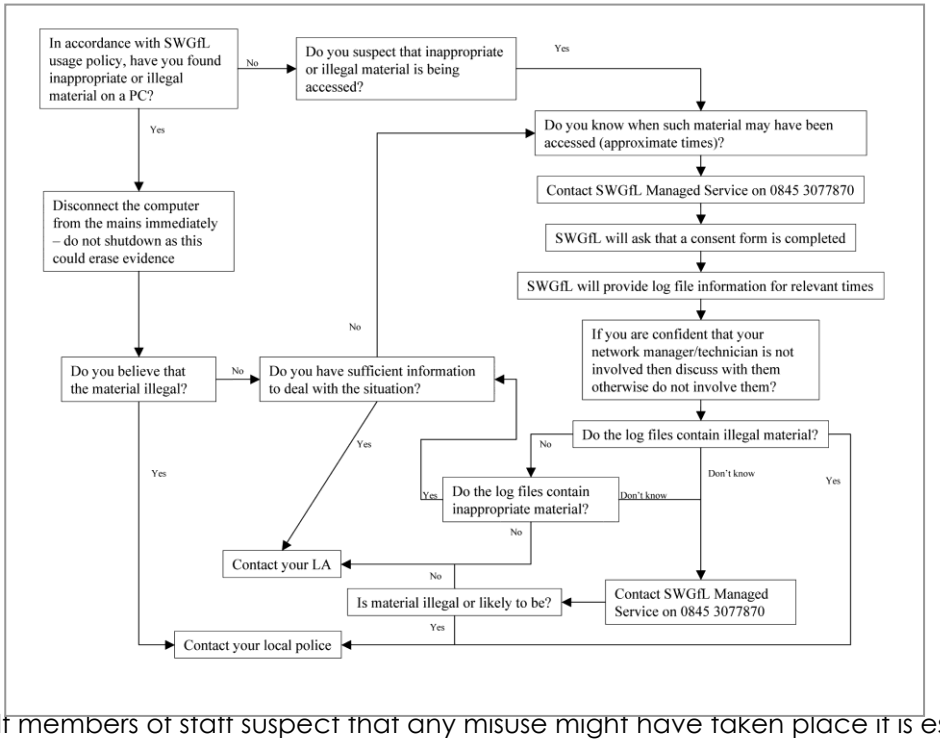
- The official school email service is used for communications between staff, and with parents/carers and students as it provides an effective audit trail.
- Any digital communication between staff and students / pupils or parents / carers (email, chat, VLE etc) must be professional in tone and content. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications.
- Users are made aware that email communications may be monitored and what to do if they receive an email that makes them feel uncomfortable, is offensive, threatening or bullying in nature through the acceptable use policies.
- Where appropriate, whole class or group email addresses will be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use only.
- Students / pupils are taught about email safety issues through the scheme of work and implementation of the acceptable use policy.
- Personal information is not sent via e-mail as this is not secure. Personal information is also not posted on the school website and only official email addresses are listed for members of staff.
- The following table shows how the school currently considers these should be used.

	Staff & other adults				Students / Pupils			
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	x						x	
Use of mobile phones in lessons				x				x
Use of mobile phones in social time		x						x
Taking photos on mobile phones or other camera devices		x					x	
Use of hand held devices e.g. PDAs, PSPs	x				x			
Use of personal email addresses in school, or on school network	x							x
Use of school email for personal emails	x							x
Use of chat rooms / facilities		x					x	
Use of instant messaging		x						x
Use of social networking sites				x				x
Use of blogs		x					x	

Responding to incidents of misuse

We expect all members of the school community to be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy take place, through careless, irresponsible or, very rarely, deliberate misuse. If any apparent or actual misuse appears to involve illegal activity the SWGfL flow chart below is consulted and followed, in particular the sections on reporting the incident to the police and the preservation of evidence. Illegal activity would include:

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials



If members of staff suspect that any misuse might have taken place it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. In such event the SWGfL "Procedure for Reviewing Internet Sites for Suspected Harassment and Distress" will be followed. This guidance recommends that more than one member of staff is involved in the investigation which should be carried out on a "clean" designated computer. It is more likely that the school will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the school community are aware that incidents have been dealt with.

Unsuitable / inappropriate activities

The school believes that the activities referred to below are inappropriate school and that users should not engage in these activities in school or outside school when using school equipment or systems.

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
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					X
	promotion or conduct of illegal acts, e.g. under child protection, obscenity, computer misuse and fraud legislation					X
	adult material that potentially breaches the Obscene Publications Act in the UK					X
	criminally racist material in UK					X
	Pornography				X	
	promotion of any kind of discrimination				X	
	promotion of racial or religious hatred				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	any other information which may be offensive to colleagues, breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business					X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SWGfL and / or the school					X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet					X	
On-line gaming (educational)		X				
On-line gaming (non educational)			X			
On-line gambling					X	
On-line shopping / commerce			X			
File sharing				X		
Use of social networking sites apart from Merlin e.g. Bebo, Facebook for older users				X		

Use of video broadcasting e.g. Youtube			X	

Students / Pupils **Actions / Sanctions**

Incidents:	Refer to class teacher / tutor	Refer to Head of Department / Head of Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X	X	X	X	X	X
Unauthorised use of non-educational sites during lessons	X								
Unauthorised use of mobile phone / digital camera / other handheld device	X	X							
Unauthorised use of social networking / instant messaging / personal email	X					X			
Unauthorised downloading or uploading of files		X				X			
Allowing others to access school network by sharing username and passwords		X	X			X			
Attempting to access or accessing the school network, using another student's / pupil's account	X	X	X			X		X	
Attempting to access or accessing the school network, using the account of a member of staff	X	X	X			X	X	X	X
Corrupting or destroying the data of other users	X	X	X		X	X	X	X	
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X	X
Continued infringements of the above, following previous warnings or sanctions		X	X	X		X	X		X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X	X	X	
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X		
Accidentally accessing offensive	X	X				X		X	

or pornographic material and failing to report the incident									
Deliberately accessing or trying to access offensive or pornographic material		X	X		X	X	X	X	
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X	X	X	X	X	X	X	X

Staff **Actions / Sanctions**

Incidents:	Refer to line managerr	Refer to Headteacher	Refer to Local Authority / HR	Refer to Police	Refer to Technical Support Staff for action	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).		X	X	X		X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X					X		
Unauthorised downloading or uploading of files	X	X				X	X	
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	X	X	X		X	X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X				X	X		
Deliberate actions to breach data protection or network security rules	X	X	X			X	X	
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X		X	X	X	X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X		X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X				X		

Actions which could compromise the staff member's professional standing	X	X	X			X	X	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X			X		
Using proxy sites or other means to subvert the school's filtering system	X	X	X		X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X							
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X			X	X	X
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Schedule for Development/Monitoring/Review

This e-safety policy was approved by the *Governing Body / Governors Sub Committee on:*	
The implementation of this e-safety policy will be monitored by the:	*School Leadership Team & E safety coordinator*
Monitoring will take place at regular intervals:	*Yearly review*
The *Governing Body / Governors Sub Committee* will receive a report on the implementation of the e-safety policy:	*Yearly (as part of ICT report)*
The E-Safety Policy will be reviewed bi-annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	*2018*
Should serious e-safety incidents take place, the following external persons / agencies should be informed:	*LA ICT Manager- currently Jo Briscombe, If appropriate-LA Safeguarding Officer, Police*

The school will monitor the impact of the policy using:

- *Logs of reported incidents*
- *SWGfL monitoring logs of internet activity (including sites visited)*
- *Surveys / questionnaires of:*
  - *Learners (eg Ofsted "Tell-us" survey / CEOP ThinkUknow survey)*
  - parents / carers
- *Staff*

Agreed By Staff.....

Agreed by Governors.....

Signed.....

Review date: May 2022

Appendix 1: Roles and Responsibilities

Role	Responsibility
Governors	• Approve and review the effectiveness of the E-Safety Policy and acceptable use policies • E-Safety Governor works with the E-Safety Leader to carry out regular monitoring of e-safety incident logs, filtering, changes to filtering and then reports to Governors
Head teacher and Senior Leaders:	• Ensure that all staff receive suitable CPD to carry out their e-safety roles and sufficient resource is allocated. • Ensure that there is a system in place for monitoring e-safety • Follow correct procedure in the event of a serious e-safety allegation being made against a member of staff • Inform the local authority about any serious e-safety issues including filtering • Ensure that the school infrastructure / network is safe and secure and that policies and procedures approved within this policy are implemented.
E-Safety Leader:	• Lead the e-safety working group and dealing with day to day e-safety issues • Lead role in establishing / reviewing e-safety policies / documents, • Ensure all staff are aware of the procedures outlined in policies • Provide and/or brokering training and advice for staff, • Attend updates and liaising with the LA e-safety staff and technical staff, • Deal with and log e-safety incidents including changes to filtering, • Meet with E-Safety Governor to regularly to discuss incidents and review the log • Report regularly to Senior Leadership Team
Curriculum Leaders	• Ensure e-safety is reflected in teaching programmes where relevant e.g. anti bullying, English publishing and copyright and is reflected in relevant policies.
Teaching and Support Staff	• Participate in any training and awareness raising sessions • Have read, understood and signed the Staff Acceptable Use Agreement (AUP) • Act in accordance with the AUP and e-safety policy • Report any suspected misuse or problem to the E-Safety Co-ordinator • Monitor ICT activity in lessons, extra curricular and extended school activities
Students / pupils	• Participate in e-safety activities, follow the acceptable use policy and report any suspected misuse • Understand that the E-Safety Policy covers actions out of school that are related to their membership of the school
Parents and carers	• Endorse (by signature) the Student / Pupil Acceptable Use Policy • Ensure that their child / children follow acceptable use rules at home • Discuss e-safety issues with their child / children and monitor their home use of ICT systems (including mobile phones and games devices) and the internet • Access the school website / Merlin in accordance with the relevant school Acceptable Use Policy. • Keep up to date with issues through school updates and attendance at events
Technical Support Provider	• Ensure the school's ICT infrastructure is secure in accordance with Becta guidelines and is not open to misuse or malicious attack • Ensure users may only access the school network through an enforced password protection policy, where passwords are regularly changed for those who access children's data

	• Inform the head teacher of issues relating to the filtering applied by the Grid • Keep up to date with e-safety technical information and update others as relevant • Ensure use of the network is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator for investigation / action / sanction. • Ensure monitoring software / systems are implemented and updated • Ensure all security updates / patches are applied (including up to date anti-virus definitions, windows updates) and that reasonable attempts are made to prevent spyware and malware.
Community Users	• Sign and follow the AUP before being provided with access to school systems.

Appendix 2: Acceptable Use Forms

Parent / Carer Permission Form

KS2
I know that my son / daughter has signed an Acceptable Use Agreement and has received, and will continue to receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

Early Years/KS1
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, and will continue to receive, online safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

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

Parent / Carers Name: _____

Pupil Name: _____

Key Stage: (EYFS (reception), KS1 or KS2) _____

Please read and sign the following:
1. 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 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.

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

3. 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 online safety.

Signed: ……..
Date: ……
I give my permission for my child to be photographed/videoed during school for educational purposes, and understand that these photos/videos might be shown on the school website.
Signed: ……
Date: ……

Pupil Acceptable Use Agreement for Early Years/KS1

This is how we stay safe when we use computers:

- I will ask my teacher if I want to use the computers or tablets.
- I will follow the teacher's instructions and I will not go onto a different activity.
- I will look after the computers and i-Pads and I will not drop them, or break them.
- I will ask for help from my teacher if I am not sure what to do or if I think I have done something wrong.
- I will tell my teacher if I see something that upsets me on the computer or tablet
- I know that if I break the rules I might not be allowed to use a computer / tablet.

Signed (child) : .....

Pupil Online Acceptable Use Agreement (KS2)

School Policy

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital 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 will have good access to digital technologies to enhance their learning and will, in return, expect the pupils to agree to be responsible users.

ACCEPTABLE USE AGREEMENT

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users.

For my own personal safety:

- I understand that FCE will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.
- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, money details etc)
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that FCE computers, laptops and tablets, and other computing equipment is only to be used for my education, and that I will not use them for personal things, or play on them, unless I have permission.
- I will not (unless I have permission) 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 use FCE computers, laptops or tablets for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have the permission of my teacher to do this.

I will act as I expect others to act toward me:

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute photos of anyone on the tablets without their permission.
- I know that the school must have filtering and monitoring systems in place, and I will not by-pass these in any way at all.
- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission. I understand that, if I do use my own devices in the school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I will not upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the filtering / security systems in place.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not use the school equipment to access any social media sites (e.g. Facebook, Snapchat, Instagram, etc), unless I have my teacher's permission.
- I will not install programmes on school computers, laptops or tablets, nor will I alter computer settings without my teacher's permission.

When using the internet for learning or play, I know that:

- I should make sure that I have permission to use the any pictures/photos or text which I paste into my own work.

- Where work is protected by copyright, I will not download copies (especially music and videos).

- When I am using the internet to find information, I must remember that the information is not always true, so I should check different websites.

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

- I understand that there could be sanctions by Mrs. Marks if I am involved in incidents of inappropriate behaviour. And, even when I am out of school I must still abide by these rules. (Examples of inappropriate behaviour would include breaking any of these rules, cyber-bullying, use of images or personal information to cause someone to be upset.)
- I understand that if I break any rules of this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This may include loss of access to the school network / internet, contact with parents, exclusion and in the event of illegal activities involvement of the police.

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school systems and devices.

STUDENT / PUPIL ACCEPTABLE USE AGREEMENT FORM

This form relates to the pupil Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, you will not be able to use the school IT technologies.

I have read and understand the above and agree to follow these guidelines when:

- I use FCE computers, laptops and tablets.
- I use my own equipment out of school.

Name of Student / Pupil: _____

Class: _____

Signed: _____

Date: _____