Firle CE Primary School

E-Safety Policy
November 2016

Firle School is committed to safeguarding and promoting the welfare of children and young people and expects all staff and volunteers to share this commitment.

Writing and reviewing the e-safety policy

E-safety is part of the school's safeguarding responsibilities. This policy relates to other policies including those for behaviour, safeguarding, anti-bullying, social media and the use of images (cameras and mobile phones).

Using this policy

- The school will appoint an e-safety coordinator. (See Appendix 1 for the role of e-safety coordinator).
- Our e-safety Policy has been written by the school, building on best practice and government guidance. It has been agreed by senior management and approved by governors.
- The e-safety policy covers the use of all technology which can access the school network and the internet or which facilitates electronic communication from school to beyond the bounds of the school site. This includes but is not limited to workstations, laptops, mobile phones, tablets and hand held games consoles used on the school site.
- The e-safety policy recognises that there are differences between the use of technology as a private individual and as a member of staff / pupil.

Teaching and learning

Why Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide students with quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary tool for staff and pupils.
- Pupils will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- Pupils will be shown how to publish and present information appropriately to a wider audience.

Pupils will be taught how to evaluate Internet content

- The school will seek to ensure that the use of Internet derived materials by staff and by pupils complies with copyright law.
- Pupils should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy.
- For pupils whose parents lack economic or cultural educational resources, the school should build digital skills and resilience acknowledging the lack of experience and internet at home
- For children with social, familial or psychological vulnerabilities, further consideration should be taken to reduce potential harm.

Managing access and security

The school will provide managed internet access to its staff and pupils in order to help pupils to learn how to assess and manage risk, to gain the knowledge and understanding to keep themselves safe when using the internet and to bridge the gap between school IT systems and the more open systems outside school

- The school will use a recognised internet service provider or regional broadband consortium.
- The school will ensure that all internet access has age appropriate filtering provided by a recognised filtering system which is regularly checked to ensure that it is working, effective and reasonable.
- The school will ensure that its networks have virus and anti-spam protection.
- Access to school networks will be controlled by personal passwords.
- Systems will be in place to ensure that internet use can be monitored and a log of any incidents will be kept to help to identify patterns of behaviour and to inform e-safety policy.
- The security of school IT systems will be reviewed regularly.
- All staff that manage filtering systems or monitor IT use will be supervised by senior management and have clear procedures for reporting issues.
- The school will ensure that access to the Internet via school equipment for anyone not employed by the school is filtered and monitored.

Managing Internet use

The school will provide an age-appropriate e-safety curriculum that teaches pupils how to stay safe, how to protect themselves from harm and how to take responsibility for their own and others' safety. Any, and all, communication between staff and pupils or families will take place using school equipment and/or school accounts. Pupils will be advised not to give out personal details or information which may identify them or their location

E-mail

- **Pupils and staff may only use approved e-mail accounts on the school system.**
- Pupils must immediately tell a teacher if they receive offensive e-mail.
- Pupils must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission.
- Staff to pupil email communication must only take place via a school email address or from within the learning platform and will be monitored.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The school will consider how e-mail from pupils to external bodies is presented and controlled.
- The forwarding of chain letters is not permitted.

Published content and the school website

- The contact details on the web site should be the school address, e-mail and telephone number. Staff or pupils' personal information will not be published.
- The head teacher, office staff and Computing coordinator will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing pupils' images and work

- Photographs that include pupils will be selected carefully and will not enable individual pupils to be identified. The school will seek to use group photographs rather than full-face photos of individual children.
- Pupils' full names will not be used on the website or learning platform, as appropriate, including in blogs, forums or wikis, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of pupils are published on the school website. Parents should be clearly informed of the school policy on image taking and publishing, both on school and independent electronic repositories.

Social networking and personal publishing on the school learning platform

- The school will control access to social networking sites, and consider how to educate pupils in their safe use e.g. use of passwords. This control may not mean blocking every site, but will certainly mean monitoring and educating students in their use.
- Use of video services such as Skype, Google Hangouts and Facetime will be monitored by staff. Pupils must ask permission from a member of staff before making or answering a video call.

- Staff and pupils should ensure that their online activity, both in school and out takes into account the feelings of others and is appropriate for their situation as a member of the school community. Pupils are taught about the consequences of cyberbullying and how it fits specifically into the school's anti-bullying ethos and policy.
- Newsgroups will be blocked unless a specific use is approved.
- Pupils will be advised never to give out personal details of any kind which may identify them or their location.
- Pupils must not place personal photos on any social network space provided in the school learning platform.
- Pupils and parents will be advised that the use of social network spaces outside school brings a range of dangers for primary aged pupils.

Managing filtering

- The school will work in partnership with East Sussex County Council to ensure systems to protect pupils are reviewed and improved.
- If staff or pupils come across unsuitable on-line materials, the site must be reported to the e-safety Coordinator.
- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.

Managing videoconferencing

- Videoconferencing will use the educational broadband network to ensure quality of service and security rather than the Internet.
- Pupils should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the pupils' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- Mobile phones and associated cameras will not be used during lessons or formal school time except as part of an educational activity. The sending of abusive or inappropriate text messages is forbidden.
- Games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering and cannot be used in the school context.
- Staff will use a school phone where contact with pupils is required.
- The appropriate use of Learning Platforms will be discussed as the technology becomes available within the school.
- Memory cards from school digital cameras will be regularly formatted.

Use of personal devices

- Personal equipment should not be used by staff to access the school IT systems
- Staff must not store images of pupils or pupil personal data on personal devices.
- Pupils will be encouraged not to bring personal devices to school (mobile phones/SMART watches etc.) and if they do they will be stored securely by the class teacher and returned at the end of the day.
- The school cannot be held responsible for the loss or damage of any personal devices used in school or for school business.

Protecting personal data

- The school has a separate Data Handling Policy. It covers the use of biometrics in school, access to pupil and staff personal data on and off site and remote access to school systems.
- Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.
- Each member of teaching staff is issued with a school laptop. Pupil and sensitive data should only be saved on this drive or the school's main server.

Cyber-Bullying

- Cyber-Bullying consists of: threats and intimidation sent to a pupil by mobile phone, email or online; harassment through repeated unwanted contact of another person; name calling online; public posting or forwarding of images without consent.
- Allegations of cyber-bullying will be handled in the same way as bullying (as seen in the anti-bullying policy).
- To raise awareness through teaching and learning targeted to the dangers of sexting.

Prevent Duty (July 2015 update)

- Suitable filtering and supervision should be in place in order to ensure children are kept safe from terrorist and extremist material when accessing the internet in school – please refer to school Prevent Policy
- Through e-safety and PSHE lessons, pupils are to be equipped with the skills and knowledge necessary to stay safe from inappropriate material online, including terrorist and extremist material.
- Every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups and will have completed the NCALT online

Channel training interactive, or had in school whole staff training by East Sussex County Council.

- Fundamental British Values are advertised and delivered to children on a regular and embedded basis, within the wider school curriculum.

Policy Decisions

Authorising Internet access

- All staff (including teaching assistants, support staff, office staff, midday supervisors, student teachers, work experience trainees, ICT technicians and governors) must read and sign the 'Staff AUP' before accessing the school IT systems.
- The school will maintain a current record of all staff and pupils who are granted access to school IT systems.
- At Key Stage 1, access to the internet will be by adult demonstration with supervised access to specific, approved on-line materials.
- At Key Stage 2, access to the internet will be with teacher permission with increasing levels of autonomy.
- People not employed by the school must read and sign a Visitor AUP before being given access to the internet via school equipment.
- Parents will be asked to sign and return a consent form to allow use of technology by their pupil.

Assessing risks

- The school will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor ESCC can accept liability for the material accessed, or any consequences of Internet access.
- The school will regularly audit ICT use to establish if the e-safety policy is adequate and that the implementation of the e-safety policy is appropriate and effective.

Handling e-safety complaints

- Complaints of Internet misuse will be dealt with by a senior member of staff according to the school's behaviour policy (Appendix 3)
- Any complaint about staff misuse must be referred to the e-safety coordinator or head teacher.
- Complaints of a child protection nature must be dealt with in accordance with school child protection procedures.
- Pupils and parents will be informed of the complaints procedure.

- Pupils and parents will be informed of consequences for pupils misusing the internet and this will be in line with the schools behaviour policy.

Community use of the Internet

- Members of the community and other organisations using the school internet connection will have signed a Visitor AUP so it is expected that their use will be in accordance with the school e-safety policy.

Communication of the Policy

Introducing the e-safety policy to pupils

- Appropriate elements of the e-safety policy will be shared with pupils
- E-safety 'SMART' rules will be posted in all networked rooms and displayed in every classroom.
- Pupils will be informed that network and Internet use will be monitored.
- Curriculum opportunities to gain awareness of e-safety issues and how best to deal with them will be provided for pupils.

Staff and the e-safety policy

- All staff will be given the School e-safety Policy and its importance explained.
- All staff must sign and agree to comply with the staff AUP.
- Staff should be aware that Internet traffic can be monitored and traced to the individual user.
- All staff will receive e-safety training on a minimum annual basis.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Enlisting parents' support

- Parents' and carers' attention will be drawn to the School e-safety Policy in newsletters, the school brochure and on the school web site.
- Parents and carers will from time to time be provided with additional information on e-safety in the form of written communications or workshop type events.
- The school will ask all new parents to sign the parent /pupil agreement when they register their child.

Policy review

- This policy will be reviewed annually and updated in line with DfE (Department for Educaton) or ESSCB (East Sussex Safeguarding Children's board) guidance or legislation.

Agreed by the Governing Body on…….

Next Review: September 2017 (Or as new guidance is released via ESSCB or the DfE)

Signed by:…….

Chair of the Governing Body

Appendix 1

The Role of the E-safety Co-ordinator.

- Complete an annual e-safety audit in conjunction with the Senior Leadership Team and/or Head

- Promote an e-safe culture under the direction of the leadership team, and promote the school's e-safety vision to all stakeholders

- Maintain the school's e-safety policy, reviewing annually

- Ensure that the e-safety policy links with other appropriate school policies e.g. Anti-Bullying, Child Protection, Computing, PSHE etc. (with the appropriate member of staff)

- Ensure the e-safety policy and its associated practices are adhered to (e.g. incident flow charts, reporting logs etc.)

- Ensure Acceptable Use Policies/school internet rules are in place, up-to-date and wherever possible are agreed by Staff, Pupils and Parents

- Work with the SENDCO and Designated Child Protection Officer to create e-safety guidance for vulnerable children and those with additional learning needs

- Manage e-safety training for all staff and ensure that e-safety is embedded within continuing professional development

- Ensure staff receive relevant information about emerging issues

- Coordinate e-safety awareness raising/education for pupils and ensure that e-safety is embedded in the curriculum, for example via e-safety schemes of work, assemblies and/or theme days

- Support e-safety awareness raising/education initiatives for parents

- Act as a point of contact, support and advice on e-safety issues for staff, pupils and parents

- Act as the first point of contact should an e-safety incident occur (particularly child protection or illegal issues), and ensure the agreed e-safety incident procedure is followed, as outlined in the school's e-safety policy

- Maintain an e-safety incident log in collaboration with the school's designated safeguarding lead

- Monitor, report and address incidences of pupils accessing unsuitable sites at school as necessary

- Keep up-to-date with local and national e-safety awareness campaigns and issues surrounding existing, new and emerging technologies

- Work with and receive support and advice from the ESSCB

Appendix 2

Staff/Governors Template Acceptable Use Policy (AUP)

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere to its contents at all times. Any concerns or clarification should be discussed with the e-safety coordinator.

- I appreciate that ICT includes a wide range of systems, including mobile phones, tablets, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner.
- I will only use the school's email / internet / intranet / Learning Platform and any related technologies for professional purposes, or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I understand that I am responsible for all activity carried out under my username.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that all electronic communications with parents, pupils and staff, including email and social networking, are compatible with my professional role and that messages cannot be misunderstood or misinterpreted.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head teacher or Governing Body.
- I will only take images of pupils and/or staff for professional purposes in line with school policy. I will not distribute images outside the school network/learning platform without the permission of the Head teacher.
- I will not install any hardware or software without the permission of the IT technician.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- I will respect copyright and intellectual property rights.

- I understand that all my use of the internet and other related technologies can be monitored and logged and can be made available, on request, to my performance manager or Head teacher.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support the school's e-safety policy and help pupils to be safe and responsible in their use of ICT and related technologies. I will promote e-safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing.
- I will report any incidents of concern regarding children's safety to the E-safety Coordinator, the Designated Safeguarding Lead / Head teacher.
- I understand that sanctions for disregarding any of the above will be in line with the school's disciplinary procedures and serous infringements may be referred to the police.

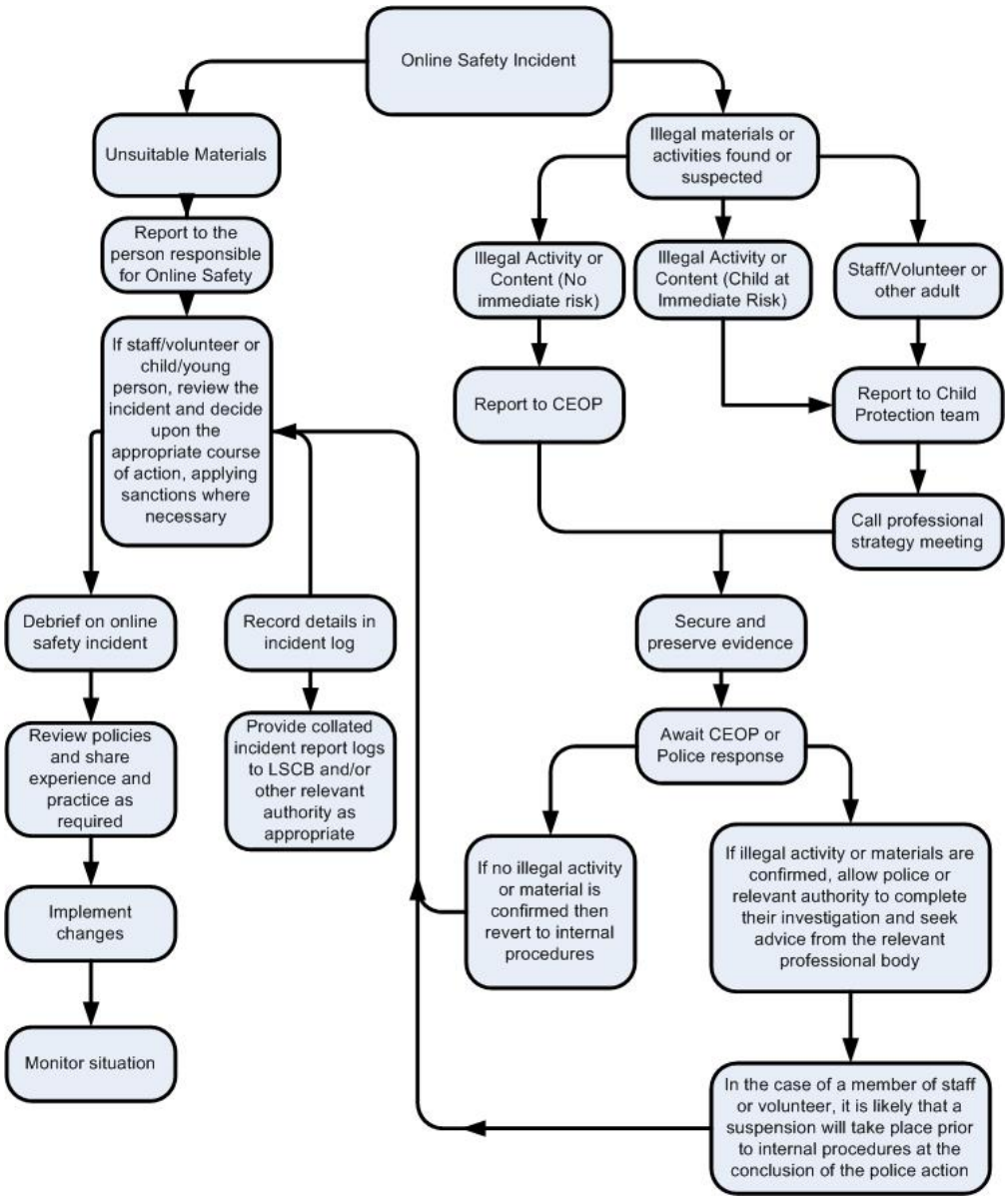
User Signature: I agree to follow this acceptable use policy and to support the safe use of ICT throughout the school.

Full Name …… (Printed)

Job Title ……

Signature…… Date……

Appendix 3


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

Appendix 4

KS1/EYS Acceptable Use Policy

This is how we stay safe when we use computers:

I will ask a teacher or suitable adult if I want to use the computers

I will only use activities that a teacher or suitable adult has told or allowed me to use.

I will take care of the computer and other equipment

I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong.

I will tell a teacher or suitable 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.

Signed (child):……

Signed (parent): ……..

Appendix 5

KS2 Acceptable Use Policy

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 Policy 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 users at risk.

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

Acceptable Use Policy Agreement

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

For my own personal safety:

- I understand that the *school* 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, financial 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 the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- 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 use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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 images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the *school*:

- 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 understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.
- I will not use social media at school.

When using the internet for research or recreation, I recognise that:

- I should 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 try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the *school* also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network /

internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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, access will not be granted to school systems and devices.

Pupil Acceptable Use Agreement Form

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, access will not be granted to school ICT systems.

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

- I use the *school* systems and devices (both in and out of school)
- I use my own devices in the *school* (when allowed) eg mobile phones, gaming devices USB devices, cameras etc
- I use my own equipment out of the school in a way that is related to me being a member of this *school* eg communicating with other members of the school, accessing school email, VLE, website etc.

Name of Student / Pupil	
Group / Class	
Signed	
Date	

Appendix 6 Parent / Carer Acceptable Use Agreement

Digital technologies have become integral to the lives of children and young people, both within schools and outside school. These technologies provide powerful tools, which open up new opportunities for everyone. They 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 Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that 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 digital technologies to enhance their learning and will, in return, expect the *pupils* to agree to be responsible users. A copy of the Pupil Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

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.

Permission Form

Parent / Carers Name | | Student / Pupil Name | |

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.

(KS2 and above)
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 use of technology and the internet – both in and out of school.

(KS1)
I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, e-safety education to help them understand the importance of safe use of technology and the internet – 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 Policy.

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.

Signed | Date