ACCEPTABLE USE OF THE INTERNET – E-SAFETY POLICY

CLAINES
CE PRIMARY SCHOOL

AT CLAINES CE PRIMARY SCHOOL, WE HAVE A STRONG COMMITMENT TO ENSURING CHILDREN FLOURISH AND SUCCEED TOGETHER AS PART OF A STRONG SCHOOL COMMUNITY. DRIVEN BY SOME OF OUR KEY VALUES OF RESPECT AND COMPASSION, WE ARE INCLUSIVE AND COMMITTED TO THE INDIVIDUAL CHILD. WE AIM FOR A SCHOOL WHERE EVERYONE IS TREATED WITH DIGNITY AND VALUED FOR THEIR PLACE IN OUR COMMUNITY AND THE WIDER WORLD. AT THE HEART OF OUR LEARNING, ARE THE VALUES OF PERSEVERANCE AND COURAGE. WE STRIVE FOR EVERYONE TO HAVE GREAT ASPIRATIONS: ENSURING NEW CHALLENGES ARE MET WITH CONFIDENCE AND 'NO ONE SETTLES FOR LESS THAN THEIR BEST'.

WE DO ALL OF THIS WHILST FOLLOWING IN THE FOOTSTEPS OF CHRIST.

Approved by:	Curriculum & Standards Committee	**Date:** 9.3.20
Last reviewed on:	9.3.20	
Next review due by:	March 2022	

CLAINES
CE PRIMARY SCHOOL

ACCEPTABLE USE OF THE INTERNET POLICY – E-SAFETY

Introduction

New technologies have become integral to the lives of children and young people in 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 pupils 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. 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
- Inappropriate communication / contact with others, including strangers
- 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.

Many of these risks reflect situations in the off-line world and it is essential that this E-safety policy is read in conjunction with other school policies (including; Behaviour Policy, Safeguarding Policy, Acceptable ICT usage statement). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build 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.

Responsibilities of the School Community

We believe that e-safety is the responsibility of the whole school community, and everyone has their part to play in ensuring all members of the community are able to benefit from the opportunities that technology provides for learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Responsibilities of the Headteacher

The Headteacher 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 Lead.

- ensuring that relevant staff receive suitable CPD to enable them to carry out their e-safety roles and to train other colleagues, as relevant. The Headteacher will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. The Headteacher and Deputy Head Teacher are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Responsibilities of the E-Safety Lead (Mr Simon Gent)

The E-safety Lead is responsible for:

- taking day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies/documents. The E-Safety Lead is supported in their role by the Designated Safeguarding Lead and Deputy Designated Safeguarding Leads, as well as all school leaders and staff within the school. E-safety is considered an active responsibility of all colleagues.
- ensuring that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place.
- providing advice for staff
- liaising with school Computing technical staff
- receiving reports of e-safety incidents and creates a log of incidents to inform future e-safety developments which are reported to the Headteacher and Governors as appropriate.

Responsibilities of Teachers and Support Staff

Teaching and support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices
- they have read, understood and signed the school Acceptable ICT Usage Statement. This is signed annually and in signing staff accept that the school can monitor network and internet use to help ensure staff and pupil safety
- they report any suspected misuse or problem to the Deputy Headteacher and Headteacher immediately for investigation/action/sanction
- e-safety issues are embedded in all aspects of the curriculum and other school activities
- they monitor Computing activity in lessons and extra-curricular school activities and provide parents with advice on safe use of Computing outside of school.
- they are aware of e-safety issues related to the use of mobile phones, cameras and handheld devices and that they monitor their use and implement current school policies with regard to these devices
- in lessons where internet use is pre-planned children should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches

Safeguarding leads and Deputy leads are trained in e-safety issues and are 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
- cyber-bullying

Responsibilities of Technical Staff

The IT Technician is responsible for ensuring:

- that the school’s Computing infrastructure is secure and is not open to malicious attack
- that users may only access the school’s networks through a properly enforced password protection policy, in which passwords are changed regularly.
- Any major filtering issues that are observed by the onsite engineer are escalated to their line manager and if required reported to Sophos.

- that he keeps up to date with e-safety technical information in order to effectively carry out their e-safety role and to inform and update others as relevant. IT technician to attend relevant staff training
- that the use of the network /remote access via the VPN is monitored in order that any misuse/attempted misuse can be reported to the E-Safety Lead and/or Headteacher immediately

Responsibilities of Pupils

- Read, understand and adhere to the school pupil AUA.
- Help and support the school in creating e-safety policies and practices; and adhere to any policies and practices the school creates.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies in school and at home.
- Take responsibility for your own and each other's safe and responsible use of technology in school and at home, including judging the risks posed by the personal technology owned and used by pupils outside of school.
- Ensure you respect the feelings, rights, values and intellectual property of others in your use of technology in school and at home.
- Understand what action you should take if you feel worried, uncomfortable, vulnerable or at risk whilst using technology in school and at home, or if you know of someone who this is happening to.
- Not to do anything online that could cause others to feel hurt or upset
- Discuss e-safety issues with family and friends in an open and honest way.

Responsibilities of Parents and Carers

- Help and support your school in promoting e-safety.
- Read, understand and promote the school pupil AUA with your children.
- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that your children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies
- Discuss e-safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviour in their own use of technology.
- Consult with the school if there are any concerns about their children's use of technology.

Responsibilities of Governing Body

Governors are responsible for the approval of the E-Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the governors receiving regular information about e-safety incidents and monitoring reports. At Claines CE Primary, a governor has taken on the role of Safeguarding Governor and this includes E-safety. The role of the E-safety Lead/Headteacher/Safeguarding Governor will be:

- regular monitoring of e-safety incident logs
- regular monitoring of filtering / change control logs

Learning and Teaching

We believe that the key to developing safe and responsible behaviour online, not only for pupils but for everyone within our school community, lies in effective education. We know that the Internet and other technologies are embedded in our pupils' lives not just in school but outside as well, and we believe we have a duty to help prepare our pupils to benefit safely from the opportunities the Internet brings.

We will provide specific e-safety related lessons in every year group as part of the Computing curriculum and PSHE curriculum.

We will celebrate and promote e-safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.

We will discuss, remind or raise relevant e-safety messages with pupils routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.

We will remind pupils about their responsibilities through an end-user AUA which every pupil will confirm when they log on.

Staff will model safe and responsible behaviour in their own use of technology during lessons.

Parental Involvement

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe. To achieve this, we will:

- include e-safety in our annual meetings with parents, and
- include useful links and advice on e-safety regularly in newsletters and on our school website.

Managing ICT Systems and Access

The school will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible.

Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access. Access to this will be permitted for the computing coordinator, Headteacher and technicians.

Servers, workstations and other hardware and software will be kept updated as appropriate.

Virus protection is installed on all appropriate hardware, and will be kept active and up-to-date.

The school will agree which users should and should not have Internet access, and the appropriate level of access and supervision they should receive.

All users will sign an end-user Acceptable Use Policy (AUA) provided by the school, appropriate to their age and access. Users will be made aware that they must take responsibility for their use of, and behaviour whilst using, the school ICT systems, and that such activity will be monitored and checked.

All pupils will access school computers using a class log-on. Pupils will abide by the school AUA at all times whether supervised by a member of staff, or working independently; they will be reminded of this agreement annually in class and when they logon to any school computer.

Members of staff will access the Internet using an individual log-on, which they will keep secure. Supply staff will use a generic logon and assembly groups use a logon with limited Staff Share access. They will ensure they log-out after each session, and not allow pupils to access the Internet through their log-on. They will abide by the school AUA at all times.

Any administrator or master passwords for school ICT systems should be kept secure and available to at least two members of staff, e.g. head teacher and computing coordinator.

The school will take all reasonable precautions to ensure that users do not access inappropriate material. However, it is not possible to guarantee that access to unsuitable material will never occur.

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. We will regularly review our Internet access provision, and review new methods to identify, assess and minimize risks.

Filtering Internet Access

The school uses a filtered Internet service. The filtering is provided through Capita IBS. The school also has Smoothwall and Futures Cloud installed on all curriculum machines, which monitors any inappropriate use of these machines. If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the e-safety coordinator.

If users discover a website with potentially illegal content, this should be reported immediately to the e-safety coordinator. The school will report this to appropriate agencies including the filtering provider, LA, and CEOP.

The school will regularly review the filtering and other security systems to ensure they meet the needs of all users.

Learning technologies in school

The school tries to be up to date in its use of learning technologies. In addition to computers we also currently use iPads, robots, digital cameras, video cameras, data logging and control equipment. We do not currently allow pupils to use mobile phones and gaming consoles in school. This section is kept under review and changes will be reported to the Governing Body.

Using E-Mail

Staff and pupils should use approved e-mail accounts allocated to them by the school, and be aware that their use of the school e-mail system will be monitored and checked.

Pupils will be reminded when using e-mail, or blogging, about the need to send polite and responsible messages, about the dangers of revealing personal information, about the dangers of opening e-mail from an unknown sender, or viewing/opening attachments.

Staff are required to use their school email for all school related communications. Communication between staff and pupils or members of the wider school community should be professional and related to school matters only.

Any inappropriate use of the school e-mail system, or the receipt of any inappropriate messages by a user, should be reported to a member of staff immediately.

Using images, video and sound

We will remind pupils of safe and responsible behaviour when creating, using and storing digital images, video and sound. We will remind them of the risks of inappropriate use of digital images, video and sound in their online activities both at school and at home. This will include issues around cyberbullying.

Staff and pupils will follow the school policy on creating, using and storing digital resources.

In particular, digital images, video and sound will not be taken without the permission of participants; images and video will be of appropriate activities and participants will be in appropriate dress; full names of participants will not be used either within the resource itself, within the file-name or in accompanying text online; such resources will not be published online without the permission of the staff/pupils involved.

If pupils are involved, relevant parental permission will also be sought before resources are published online.

Using blogs for pupils to publish content online

We use blogs to publish content online to enhance the curriculum by providing learning and teaching activities that allow pupils to publish their own content. However, we will ensure that staff and pupils take part in these activities in a safe and responsible manner.

Blogging, podcasting and other publishing of online content by pupils will take place within the school blogging platform (WordPress). Children, under supervision from school staff, may post on WordPress, Twitter, or Padlet.

Any public blogs run by staff on behalf of the school will be hosted on the school website and postings should be approved by class teachers, the Headteacher, or E-safety Coordinator before publishing.

Pupils will model safe and responsible behaviour in their creation and publishing of online content on the school website.

Staff and pupils will be encouraged to adopt similar safe and responsible behaviour in their personal use of blogs, wikis, social networking sites and other online publishing outside of school. Teaching of safe practice online will be taught in each year group.

Using video conferencing and other online video meetings

We use video conferencing to enhance the curriculum by providing learning and teaching activities that allow pupils to link up with people in other locations and see and hear each other. However, we will ensure that staff and pupils take part in these opportunities in a safe and responsible manner.

All video conferencing activity will be supervised by a suitable member of staff.

Pupils will not operate video conferencing equipment, or answer calls, without permission from the supervising member of staff.

Video conferencing equipment will be switched off and secured when not in use / online meeting rooms will be closed and logged off when not in use.

Pupils will be given appropriate user rights when taking part in an online meeting room. They will not have host rights or the ability to create meeting rooms.

Video conferencing should not take place off school premises without the permission of the head teacher.

Video conferences should only be recorded where there is a valid educational purpose for reviewing the recording. Such recordings will not be made available outside of the school.

Permission will be sought from all participants before a video conference is recorded.

Mobile Phones

Pupils should not generally bring a mobile phone to school. In the event of an older pupil walking to and from school alone they may carry a mobile phone if this is their parents' wish. The mobile phone should then be switched off all the time the pupil is in school and kept in the teacher's desk. We do not accept responsibility for mobile phones brought into school.

Staff mobile phones should generally be switched off or on silent during lesson times. When on a trip, staff will use their mobile phones to keep in contact with school, or during a critical incident. Staff are discouraged from giving their personal mobile phone numbers to non-members of the school staff.

Using New Technologies

As a school we will keep abreast of new technologies and consider both the benefits for learning and teaching and also the risks from an e-safety point of view.

We will regularly amend the e-safety policy to reflect any new technology that we use, or to reflect the use of new technology by pupils which may cause an e-safety risk.

Protecting Personal Data

We will ensure personal data is recorded, processed, transferred and made available according to the General Data Protection Regulations 2018.

Staff will ensure they properly log-off from a computer terminal after accessing personal data.

Staff will not remove personal or sensitive data from the school premises without permission of the headteacher, and without ensuring such data is kept secure.

The school website and other online content published by the school

The public areas of the school website will not include the personal details, including individual e-mail addresses or full names, of staff or pupils.

All content included on the school website and social media will be approved by the head teacher before publication.

Staff and pupils should not post school-related content on any external website without seeking permission first.

Dealing With e-safety Incidents

All e-safety incidents will be taken seriously. An e-safety incident could include any of the following:

- accessing illegal content deliberately;
- accessing inappropriate content deliberately ;
- accessing illegal content accidentally and failing to report this ;
- accessing inappropriate content accidentally and failing to report this;
- inappropriate use of personal technologies (e.g. mobile phones) at school ;
- accessing social networking sites, chat sites, instant messaging accounts or personal email where not allowed;

- accessing other non-educational websites (e.g. gaming or shopping websites) in school ;
- downloading or uploading files where not allowed;
- sharing your username and password with others;
- accessing school ICT systems with someone else's username and password;
- opening, altering, deleting or otherwise accessing files or data belonging to someone else;
- using school or personal equipment to send a message, or create content, that is offensive or bullying in nature;
- attempting to circumvent school filtering, monitoring or other security systems;
- sending messages, or creating content, that could bring the school into disrepute ;
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission, and
- use of online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarising of online content).

In addition for adults it could also include:

- transferring personal data insecurely
- using digital communications to communicate with pupils in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites) , and
- failure to abide by copyright of licensing agreements (for instance, using online resources in lessons where permission is not given).

Where children are concerned dealing with most safety incidents will fall within the remit of the school Behaviour Policy. In all but very minor incidents this will involve talking to a child's parents. In exceptional cases the Local Safeguarding Board or the police could be involved. Any such incident will be reported to the Governing Body.

Deliberate acts by adults that lead to an e-safety incident are unacceptable and will be treated as a disciplinary issue. If abuse is found to be repeated, flagrant or habitual, the matter will be treated as a very serious disciplinary issue. The Governors will be advised and the LA will be consulted.

Use of the School Internet by Visitors and Guests

Members of school staff will take responsibility for the actions of any adult guests or visitors whom they allow or encourage to use the school internet facilities. The essential "dos and don'ts" will be explained to such visitors and guests prior to their use of the Internet. Unacceptable use will lead to the immediate withdrawal of permission to use the school Internet facility.

Guest logins will be provided for supply teachers, students, etc who may need access to the school network.

Copyright Issues

It is recognised that all materials on the Internet are copyright, unless copyright is specifically waived. It is the school's policy that the copyright of Internet materials will be respected. Where materials are published on the Internet as part of the teacher's professional duties, copyright will remain with the County Council. Internet published materials will contain due copyright acknowledgements for any third-party materials contained within them.

Pupil (KS1)

This is how we stay safe when we use computers:

- I will ask an adult if I want to use the computer
- 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 turn off the monitor 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:	

Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Claines CE Primary 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 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 only use my own personal device if I have permission and use it within the agreed rules.
- 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, gaming 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:	

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 not use personal email addresses on the school ICT systems except in an emergency (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 School / LA Personal Data Policy (see e-security 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:	