Created by Miss Layton: February 2014

Reviewed by Miss Layton: November 2016

Handale Primary School E-Safety Policy

Designated Safeguarding Lead (DSL): Mrs Helen Blakely (Head teacher)

Designated Deputy Safeguarding Lead: Mrs Claire McGregor (2017-18)

Safeguarding Governor: Mr Darren Fowler

E-safety coordinator: Miss Lauren Layton

At Handale, ALL staff has responsibility for ALL online safety!

A quick E safety definition

E-safety encompasses a wide array of concepts and issues including:

- Copyright awareness
- Cyber-bullying
- Safe social networking and digital communication
- Digital footprint

E-safety is concerned with ensuring students use electronic resources safely and legally.

Our e-safety goals

- To protect and educate pupils and staff in their use of technology.
- To have appropriate mechanisms to intervene and support any incident where appropriate.

Ofsted recommendations

Audit:

Audit the training needs of staff and provide training to improve the knowledge and expertise in the safe and appropriate use of technology.

Families:

Work closely with all families to ensure that their children use new technologies safely and responsibly both at home and in school.

Systematic Review:

Annually review policies and practice

Managed Systems:

Manage the transition from 'locked down' to 'managed access'. Helping students understand and manage risk.

Background and rationale

The potential that technology has to impact on the lives of all citizens increases year on year. This is probably even more true for children, who are generally much more open to developing technologies than many adults. In many areas technology is transforming the way that schools teach and that children learn. At home, technology is changing the way children live and the activities in which they choose to partake; these trends are set to continue. While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- 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
- Radicalisation

The potential for excessive use, which may impact on social and emotional development and learning. This policy sets out how we strive to keep children safe with technology while they are in school. We recognise that children are often more at risk when using technology at home (where we have no control over the technical structures we put in place to keep them safe) and so this policy also sets out how we educate children of the potential risks. We also explain how we attempt to inform those people who work with our children beyond the school environment (parents, friends and the wider community) to be aware and to assist in this process.

Policy and leadership

This section begins with an outline of the key people responsible for developing our E-Safety Policy and keeping everyone safe with ICT. It also outlines the core responsibilities of all users of ICT in our school. It goes on to explain how we maintain our policy and then to outline how we try to remain safe while using different aspects of ICT.

Responsibilities of Governing bodies

Filters and Monitoring

Governing bodies and proprietors should be doing all that they can to limit children's exposure to the above risks from the school's system. As part of this process, governing bodies should ensure their school has appropriate filters and monitoring systems in place. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies should consider the age range of their pupils, the number of pupils, how often they access the IT system and proportionality of cost vs risks.

Responsibilities of the e-safety coordinator (Miss Layton)

Miss Layton is our e-safety coordinator and is the person responsible to report to the head teacher and governors, alongside the DSL (Mr Ledger) for the day-to-day issues relating to e-safety. The e-safety coordinator:

•Takes day-to-day responsibility for e-safety issues and has a leading role in establishing and reviewing the school e-safety policies / documents.

•Ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident.

•Provides training and advice for staff.

•Liaises with the Local Authority

•Liaises with school ICT technical staff

•Receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments

•Reports regularly to Senior Leadership Team

•Receives appropriate training and support to fulfil their role effectively

•Has responsibility for blocking / unblocking Internet sites in the school's filtering system / passing on requests for blocking / unblocking to the ICT Helpdesk.

•Maintains logs of any occasions where the school has used its powers of search and deletion of electronic devices.

Reports to governors.

Responsibilities of the Head Teacher (Mrs Blakeley)

•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 Co-ordinator

•The head teacher and another member of the senior management team (DSL) should be aware of the procedures to be followed in the event of a serious e-safety allegation being

made against a member of staff. see flow chart on dealing with e-safety incidents – below and relevant Local Authority HR / disciplinary procedures)

Responsibilities of classroom based staff

Classroom based staff; Teaching and Support Staff are responsible for ensuring that:

•They have an up to date knowledge of e-safety matters and of the current school e-safety policy and practices

•They have read, understood and signed the school's Acceptable Use Policy for staff

•They report any suspected misuse or problem to the E-Safety Co-ordinator

•Digital communications with students (email / Virtual Learning Environment (VLE) / voice) should be on a professional level and only carried out using official school systems

•Safety issues are embedded in the curriculum and other school activities and all staff have responsibility for ALL online safety.

Responsibilities of ICT technician

The technician must ensure that systems comply with DFE data and infrastructure guidance and cloud bared systems guidance.

The ICT Technician is responsible for ensuring that:

•The school's ICT infrastructure is secure and is not open to misuse or malicious attack

•Users may only access the school's networks through a properly enforced password protection policy

•Shortcomings in the infrastructure are reported to the ICT coordinator or head teacher so that appropriate action may be taken.

Policy Scope

This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school ICT systems, both in and out of school. The Education and Inspections Act 2006 empowers head teachers, to such extent as is reasonable, to regulate the behaviour of 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 of cyber-bullying, or other e-safety incidents covered by this policy, which may take place out of school, but is 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, where known, inform parents / carers of incidents of inappropriate e-safety behaviour that take place out of school.

Acceptable Use Policies

All members of the school community are responsible for using the school ICT systems in accordance with the appropriate acceptable use policy, which they will be expected to sign

before being given access to school systems. Acceptable use policies are provided in Appendix 1 of this policy for:

•Pupils (EYFS + KS1 / KS2)

•Staff (and volunteers)

•Parents / carers (including permissions to use pupil images / work and to use ICT systems)

Copies are sent home for further discussion with parents. For children in EYFS and KS1 parents may sign on behalf of their children Staff and volunteers sign when they take up their role in school and in the future if significant changes are made to the policy Parents sign once when their child enters the school. The parents' policy also includes permission for use of their child's image (still or moving) by the school, permission for their child to use the schools ICT resources (including the internet) and permission to publish their work. A copy of the pupil AUP is made available to parents at this stage and at the beginning of each year. Community users sign when they first request access to the school's ICT system. Induction policies for all members of the school community include this guidance.

Whole School approach and links to other policies

This policy has strong links to other school policies as follows:

Core ICT Policies:

ICT Policy: How ICT is used, managed, resourced and supported in our school.

E-Safety Policy: How we strive to ensure that all individuals in school stay safe while using ICT. The e- safety policy constitutes a part of the ICT policy.

ICT Progression and covering the ICT Curriculum. (Refer to ICT Whole School Panning).

Other policies relating E safety

Anti bullying: How our school strives to PREVENT bullying – link to cyber bullying PSHE e-Safety has links to this – staying safe.

Safeguarding: Safeguarding children electronically is an important aspect of E-Safety. The e-safety policy forms a part of the school's safeguarding policy

Behaviour: Linking to positive strategies for encouraging e-safety and sanctions for disregarding it.

Illegal or inappropriate activities and related

The school believes that the activities listed below are inappropriate in a school context (those underlined are illegal) and that users should not engage in these activities when using school equipment or systems (in or out of school). 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 (The Protection of Children Act 1978)
- Grooming, incitement, arrangement or facilitation of sexual acts against children (Illegal Sexual Offences Act 2003).
- Possession of extreme pornographic images (Illegal Criminal Justice and Immigration Act 2008).
- Criminally racist material in UK to stir up religious hatred on the grounds of sexual orientation. (Public Order Act 1986)
- Pornography
- Promotion of any kind of discrimination
- Promotion of racial or religious hatred
- Threatening behaviour, including promotion of physical violence or mental harm

Any other information, which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute Additionally the following activities are also considered unacceptable on ICT kit provided by the school:

- Using school systems to run a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Herefordshire Council and / or the school
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)
- Creating or propagating computer viruses or other harmful files
- 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
- On-line gambling and non-educational gaming
- Use of personal social networking sites / profiles for non-educational purposes

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (see above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. 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. It is intended

that incidents of misuse will be dealt with through normal behaviour / disciplinary procedures as decided by the E-safety coordinator in school and the head teacher.

Use of hand held technology (personal phones and hand held devices)

We recognise that the area of mobile technology is rapidly advancing and it is our school's policy to review its stance on such technology on a regular basis. Currently our policy is this:

Members of staff are permitted to bring their personal mobile devices into school. They are required to use their own professional judgement as to when it is appropriate to use them. Broadly speaking this is:

- Personal hand held devices will be used in lesson time only in an emergency or extreme circumstances
- Members of staff are free to use these devices in school, outside teaching time.

Pupils are not currently permitted to bring their personal hand held devices into school.

Email

- Access to email is provided for all staff in school via office365. These official school email services may be regarded as safe and secure and are monitored.
- Staff and pupils should use only the school email services to communicate with others when in school, or on school systems (eg by remote access).
- Users need to be aware that email communications may be monitored.
- Pupils can have access to an individual email account for communication within school.
- A structured education programme is delivered to pupils which helps them to be aware of the dangers of and good practices associated with the use of email.
- Staff may only access personal email accounts on school systems for emergency or extraordinary purposes (these may be blocked by filtering).
- Users must immediately report, to their class teacher / e-safety coordinator – in accordance with the school policy the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.

Use of digital and video images

- When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Members of staff are allowed to take digital still and video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be captured using school equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital / video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission

See also the following section for guidance on publication of photographs

Use of web-based publication tools

- Our school uses the public facing website, www.handaleprimary.co.uk for sharing information with the community beyond our school. This includes, from time-to-time celebrating work and achievements of children.
- All users are required to consider good practice when publishing content.
- Personal information should not be posted on the school website and only official email addresses (provided as links rather than appearing directly on the site) should be used to identify members of staff (never pupils).
- Only pupil's first names are used on the website, and only then when necessary.
- Detailed calendars are not published on the school website.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with the following good practice guidance on the use of such images:
- Pupils' full names will not be used anywhere on a website or blog, and never in association with photographs.

Professional standards for staff communication

In all aspects of their work in our school teachers abide by the Teachers' Standards as described by the DfE (http://media.education.gov.uk/assets/files/pdf/t/teachers%20standards.pdf . Teachers translate these standards appropriately for all matters relating to e-safety. Any digital communication between staff and pupils or parents / carers (email, etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications. Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice. The views and experiences of pupils are used to inform this process also.

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

The day-to-day responsibility for the management of the school's filtering policy is held by the provider, governors and DSL (with ultimate responsibility resting with the head teacher and governors). They manage the school filtering, in line with the processes outlined below and keep logs of changes to and breaches of the filtering system.

All users have a responsibility to report immediately to class teachers / e-safety coordinator any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should be blocked.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Education / training / awareness

Pupils are made aware of the importance of filtering systems through the school's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the AUP (a part of their induction process)
- briefing in staff meetings, training days, memos etc. (from time to time and on-going).
- Parents will be informed of the school's filtering policy through the Acceptable Use agreement and through e-safety awareness sessions / newsletter etc.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment.

E-safety education

Whilst regulation and technical solutions are very important, their use must be balanced by educating pupils to take a responsible approach. The education of pupils in e-safety is therefore an essential part of the 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. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of ICT, PHSE and other lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school. E-safety is also fully embedded as part of the computing curriculum and should be delivered by all class teachers.
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/ (Hectors World at KS1 and Cyber CafJ at KS2)
- Learning opportunities for e-safety are built into the curriculum.
- Key e-safety messages should be reinforced through further input via assemblies and pastoral activities as well as informal conversations when the opportunity arises.
- Pupils should be helped to understand the need for the pupil AUP and encouraged to adopt safe and responsible use of ICT both within and outside school.
- In lessons where Internet use is pre-planned, it is best practice that pupils 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.
- Where pupils are allowed to freely search the Internet, e.g. using search engines, staff should be vigilant in monitoring the content of the websites the young people visit.

In day to day school life we must ensure that e-safety is taught throughout the curriculum. How this can be done is detailed in the computing and e-safety report written by Miss Layton in November 2016. At Handale we also cover specific aspects of E-safety in each year group to ensure children receive a broadened education regarding different aspects of E-safety. The decided curriculum is reviewed on a regular basis to meet the needs of the children and current trends. The E-safety curriculum is as follows:

Year Group	E-safety Issue	Suggested Ideas
Year 2	Safe gaming	Focus on games that are over the internet. Discuss their dangers. What games are children playing on? (Xbox live, play station, moshi monsters, etc)
Year 3	Secure password Cyber bullying	At the start of the year, children should be taught about secure passwords and create one for their school account to use throughout their school lives. Discuss why is a secure password important? What is cyber bullying? How do people cyber bully? What do they use? Show videos on cyber bullying.
Year 4	Safe social networking and digital communication	What is social networking? How can we ensure that social networking stays safe? What information should we share? What are the positive aspects to social networking?

		(Discuss grooming – people have a hidden agendas and are not always who they say they are). Show children cases in the news of incidents were people have abused the trust of social networking.
Year 5	Facebook	Discuss both the dangers and benefits of facebook. What can facebook be good for? (Communication with friends/family who don't live near by, etc) What can it be bad for? (Cyber bullying, job interviews, etc). Get children, if willing, to get their facebook account up on the whiteboard. What information can people get from it? How would this appear to a person interviewing you for a job? Can people find out where you live? Discuss and check children's security settings. Show video about information put on facebook.
Year 6	Sexting Digital Footprint	What is sexting? What is your digital footprint? Discuss issues surrounding both. (identity theft, problems with getting a job due to what is on the internet, etc).

Teachers must cover their particular area of e-safety during Internet safety day. They must plan activities and provide information to children about the area concerned.

Information literacy

- Pupils should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information by employing techniques such as: Checking the likely validity of the URL (web address), Cross checking references (can they find the same information on other sites), Checking the pedigree of the compilers / owners of the website.
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make best use of internet search engines to arrive at the information they require
- We use the resources on CEOP's Think U Know site as a basis for our e-safety education http://www.thinkuknow.co.uk/teachers/resources/

The contribution of the children to e-learning strategy

It is our general school policy to require children to play a leading role in shaping the way our school operates and this is very much the case with our e-learning strategy. Children often use

technology out of school in ways that we do not in school and members of staff are always keen to hear of children's experiences and how they feel the technology, especially rapidly developing technology (such as mobile devices) could be helpful in their learning. Pupils play a part in monitoring this policy.

Staff training

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal e-safety training will be made available to staff. An audit of the e-safety training needs of all staff will be carried out regularly.
- Regular updates using email, message boards etc.
- It is expected that some staff will identify e-safety as a training need within the performance management process.
- All new staff should receive e-safety training as part of their induction programme, ensuring that they fully understand the school e-safety policy and acceptable use policies which are signed as part of their induction
- The E-Safety Coordinator will receive regular updates through attendance at local authority or other information / training sessions and by reviewing guidance documents released by the DfE, local authority and others.
- All teaching staff have been involved in the creation of this e-safety policy and are therefore aware of its content.
- The E-Safety Coordinator will provide advice, guidance and training as required to individuals as required on an on-going basis.

Parent and carer raising awareness

Many parents and carers have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring and regulation of the children's on-line experiences. Parents often either underestimate or do not realise how often children and young people come across potentially harmful and inappropriate material on the internet and are often unsure about what they would do about it. "There is a generational digital divide". (Byron Report).

The school will therefore seek to provide information and awareness to parents and carers through:

- Letters, newsletters, web site
- Parents evenings
- Reference to the parents materials on the Think U Know website (www.thinkuknow.co.uk) or others

Wider school community understanding

The school will offer family learning courses in ICT, media literacy and e-safety so that parents and children can together gain a better understanding of these issues. Messages to the public around e safety should also be targeted towards grandparents and other relatives as well as parents. Everyone has a role to play in empowering children to stay safe while they enjoy these new technologies, just as it is everyone's responsibility to keep children safe in the non-digital world.

Community Users who access school ICT systems and website as part of the Extended School provision will be expected to sign a Community User AUP before being provided with access to school systems.

HANDALE Acceptable use policy agreement KS1 Pupil

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 that an adult says are 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 understand these computer rules and will do my best to keep them.

Name of Pupil:	
Date:	

Acceptable use policy agreement – pupil (KS2)

I understand that while I am a member of Handale 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, wherever possible be supervised and monitored.
- I understand that my use of the internet will be 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 ICT kit if I have permission and then I will use it within the agreed rules.
- I will not deliberately bypass any systems designed to keep the school safe (such as filtering of the internet).
- 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 on ICT devices belonging to the school unless I have permission.
- I will only use social networking, gaming and chat through the sites the school allows

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 of Pupil:	
Date:	

Acceptable use policy agreement – staff & volunteer

Technology has transformed learning, entertainment and communication for individuals and for all organizations 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 (laptops, email, hand held device etc) 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 anyone else's username and password.

I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, 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, unless I have permission to do so. Where these images are published (e.g. on the school website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will only communicate with pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- 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 and then in the same way 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
- 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 programs.
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.

- 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 programs 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 programs of any type on a machine, or store programs 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. Where personal data is transferred outside the secure school network, it must be encrypted.
- 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.
- I will use social media responsibly and professionally and follow the social media policy.

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 Policy 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 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 Policy 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 policy.

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 and Volunteer Name:	
Signature:	
Date:	

Acceptable use policy agreement and permission forms – parent/carer

Technology has transformed learning, entertainment and communication for individuals and for all organizations that work with young people. However, the use of technology can also bring risks. All users should have an entitlement to safe internet access at all times. This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using ICT (especially the internet).
- that school ICT 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 ICT to enhance their learning and will, in return, expect them to agree to be responsible users.
Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Name of child:	
Parents Name:	
Signature:	
Date:	

Permission for my child to use the Internet and electronic communication

As the parent / carer of the above pupil(s), I give permission for my son / daughter to have access to the internet and to ICT systems at school.
I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.
I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.
I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about any possible breaches of the Acceptable Use 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.

Permission to use digital images (still and video) of my child

The use of digital images (still and video) plays an important part in learning activities. Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.
Images may also be used to celebrate success through their publication in newsletters, on the school website and occasionally in the public media.
The school will comply with the Data Protection Act and request parents / carers permission before taking images of members of the school. We will also ensure that when images are published that the young people cannot be identified by name.
As the parent / carer of the above pupil, I agree to the school taking and using digital images of my child(ren). I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the school.
I agree that if I take digital or video images at school events, where permitted, which include images of children I will abide by these guidelines in my use of these images.

Permission to publish my child's work (including on the internet)
It is our school's policy, from time to time, to publish the work of pupils by way of celebration. This includes on the internet; via the school website and in the school's virtual learning environment (VLE)
As the parent / carer of the above child I give my permission for this activity.

Name of Parent:	
Name of child:	
Signature:	
Date:	

Your agreement of consent will carry through the school. If your circumstances change it is your responsibility to inform the school.
Our school's e-safety Policy, which contains this Acceptable Use Policy Agreement, and the one signed by your child (to which this agreement refers), is available on the school website.

Guidance for Reviewing Internet Sites

This guidance is intended for use when the school needs to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might typically include cyber-bullying, harassment, anti-social behavior and deception. These may appear in emails, texts, social networking sites, messaging sites, gaming sites or blogs etc. Do not follow this procedure if you suspect that the web site(s) concerned may contain child abuse images. If this is the case please refer to the Flowchart for responding to online safety incidents and report immediately to the police. Please follow all steps in this procedure:

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

If it does then appropriate action will be required and could include the following:

- Internal response or discipline procedures
- Involvement by Local Authority or national / local organisation (as relevant).
- Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- Isolate the computer in question as best you can. Any change to its state may affect a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the group, possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

Relevant legislation:

Education Act 1996
Education and Inspections Act 2006
Education Act 2011 Part 2 (Discipline)
The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
Health and Safety at Work etc. Act 1974
Obscene Publications Act 1959
Children Act 1989
Human Rights Act 1998
Computer Misuse Act 1990
This is not a full list of Acts involved in the formation of this advice. Further information about relevant
legislation can be found via the above link to the DfE advice document.
Keeping children safe in education (KCSIE) 2016