E-Safety and Social Networking Policy

The internet is an integral part of the 21st Century life for education and social interaction. Heathfield School has a duty to provide pupils with quality internet access as part of their learning experiences. It is the duty of the school to ensure that all pupils are provided with an appropriate education that enables them to better understand the potential dangers when using ICT

This policy will be reviewed annually.

Introduction:

Heathfield School is a special school which provides an appropriate education for pupils aged 4-11 with severe and moderate learning difficulties. Some pupils have autism spectrum disorder or social and emotional difficulties which impacts on their understanding of the world around them.

- The e-safety policy relates to other policies including those for ICT, anti-bullying and for child protection.
- The school's E-Safety Co-Ordinator is the Computing Co-Ordinator. The Head Teacher is the Designated Child Protection Officer along with members of SLT. The Computing Co-Ordinator is responsible for keeping up to date with new technologies and build awareness with stakeholders about how they can remain safe. Online safety concerns may cross over with the child protection threshold so the DSL will work with the Computing Co-Ordinator – the role of the DSL is outlined in the Safeguarding Policy.
- Guidelines have been put in place to protect pupils, staff and parents / carers when using technology and devices from the potential dangers of electronic communication.
- 'Keeping children safe in education' 2016 highlights online safety as a safeguarding issue for schools and therefore it must be considered and implemented within the school's statutory safeguarding responsibilities.

The statutory responsibilities associated with online safety include the need for all staff to be aware of the role of technology within:

- Sexual and emotional abuse
- Child Sexual Exploitation
- Radicalisation
- Abuse that can be perpetrated by children themselves and specifically identifies sexting and cyberbullying

The Early Years Foundation Stage Framework 2017 highlights that Early Years settings should ensure that children are taking steps to understand and explore the world around them – this includes the use of technology.

The school has a statutory responsibility to ensure that online safety is included within safeguarding and is referenced in other polices including the Child Protection, Safeguarding Policy Anti-Bullying, Home School agreement, Behaviour and the School Development Plan. The school has a responsibility to ensure that staff are trained sufficiently and that children are taught to understand the importance of keeping safe online.

Safeguarding, including online safety, is the responsibility of everybody who works within the school.
The school is responsible for ensuring that:

- **Appropriate filtering and monitoring of internet access is in place**
- **All members of staff receive appropriate training and guidance**
- **The curriculum prepares children for the digital world**

Staff will need regular training on new technologies and the school should undertake risk assessments for any new technologies they are considering introducing as a communication or for teaching and learning

Internet use for children and young people with SEN:

Children with SEN are potentially more vulnerable and at more risk than others when using ICT
Vulnerable children are more likely to take risks in real life as well as online therefore there needs to be careful consideration around the support and education provided to these pupils, their teachers and carers

- Pupils with ASD may take literal interpretations of content which will affect how they respond
- Pupils may not understand some of the terminology used
- Pupils with more complex needs do not always understand the concept of friendships and can trust everyone implicitly. They do not know how to make judgements about what information is safe to share
- Some pupils will be vulnerable to bullying through the internet, or may not be able to recognise they are being bullied
- Pupils may not understand how their own online behaviour could be misconstrued by another person as bullying
- Pupils may not be able to distinguish between content found online that is and is not appropriate for them

Teaching and Learning:

ICT is an integral part of children's education and it is part of the statutory curriculum. It is a necessary tool for staff, pupils and parents / carers. Online Safety forms an important part of the Heathfield Computing Curriculum and highlights the importance for children to use technology safely and respectfully, understanding how to keep personal information private and be able to identify where to go for help and support when they have concerns about content.

- Children need to learn digital literacy skills and to refine their own publishing and communications with others via the Internet

- Respect for copyright and intellectual property rights, and the correct use of published material should be taught
- Awareness of the dangers and consequences of using the Internet inappropriately should be taught
- Children need to develop an understanding on how to become safe and responsible online – this should be developed within an appropriate PSHE curriculum
- Whilst the Computing curriculum will form an essential part of online safety education, safe and responsible use of technologies must be embedded throughout the whole school curriculum to ensure children develop the required range of digital literacy and safety skills as well as develop online resilience to enable them to become safe and responsible Internet users

Heathfield School ensures that:

- The school internet access is designed expressively for pupil use and includes filtering appropriate to the needs of the pupils
- Pupils will be taught what is acceptable use of the internet with clear objectives given for pupils using the internet
- Parents / carers will be supported by information on safe use of the internet for their families where applicable and a link of useful resources on our school website
- Pupils will be supervised at all times when using ICT and the internet
- Annual engagement with the Safer Internet Day, revisiting the school's E-Safety Rules and supporting parents with developing their awareness of the important role keeping safe online plays in their child's education

Pupils will be taught how to evaluate internet content when the internet is used for learning opportunities

- The school ensures that the use of internet derived materials by staff and pupils complies with copyright law
- Staff will consider potential dangers that pupils may encounter when using the internet for specific tasks and activities (for example; a teacher will closely examine website content as part of their preparation for a lesson to ensure all content is appropriate for the pupils to access)
- Pupils will be taught how to report unpleasant internet content to their class teacher, LSA, parent or carer
- Staff will take responsibility for ensuring unpleasant internet content is reported to the Head Teacher and ICT Co-ordinator where a decision will be made regarding blocking the website if is it deemed inappropriate
- In some instances "pink slips" will be used to record concerns that may arise as a result of a pupil viewing inappropriate content and discussions with parents / carers may take place

Responsibilities of all staff:

All staff have a responsibility for safeguarding children on and offline. Their key responsibilities are:

- Contributing to the development of online safety policies
- Reading and adhering to Acceptable Use Policies (AUPs)

- Taking responsibility for the security of school/ setting systems and data
- Having an awareness of how to keep safe online, the range of different ways online safety can be compromised how they relate to safeguarding children. This should include sexting and cyberbullying.
- Modelling good practice when using new and emerging technologies
- Embedding online safety education in the curriculum delivery wherever possible
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures
- Knowing when and how to escalate online safety issues, internally and externally
- Maintain a professional level of conduct in their personal use of technology, both on and off site.
- Taking personal responsibility for professional development in this area.

Furthermore, school staff have a responsibility in managing the technical environment. This is an essential role which establishes and maintains a safe online environment. All staff should:

- work closely with the school leaders, designated safeguarding lead as well as pastoral and curriculum staff (where appropriate) to provide expertise relating to appropriate education use of ICT systems and also to ensure that learning opportunities are not unnecessarily restricted by technical safety measures.
- be clear about the procedures they must follow if they discover, or suspect, online safety incidents through monitoring of network activity and the need for these issues to be escalated immediately to the DSL and/or Headteacher/manager in line with existing school/setting safeguarding policies.

The school's ICT technician has the responsibility to:

- Ensure that an external service provider upholds the online safety practices including referring any concerns to the online safety Co-Ordinator or Senior Leadership Team.
- Ensure that the school network is monitored and any concerns reported to the DSL
- Develop an understanding of the relevant legislation
- Ensure that the school's ICT infrastructure is secure but not so secure that it gets in the way of learning.
- Ensure that appropriate anti-virus software and system updates are installed and maintained on all electronic devices.

Responsibilities of Children:

Any children using ICT should take responsibility and ownership of any online safety rules and policies as appropriate to their ability.

- Read the school Acceptable Use Policy and adhere to them
- Read, and embed the School's E-Safety Rules as part of their learning
- Respect the feelings and right of others both online and offline
- Seek help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues

- Take responsibility for keeping themselves and others safe online
- Take responsibility for understanding risks posed by new technologies
- Assess the personal risk of using any particular technology and behave safely and responsibly to limit those risks.

Responsibilities of parents / carers

Parents and Carers should:

- Read the school Acceptable Use Policy, and encourage themselves and their children to adhere to them
- Discuss online safety issues with their children, supporting the school in their online safety approaches, and reinforcing appropriate safe online behaviours at home
- Role model safe and appropriate uses of technology and social media
- Identify changes in behaviour that could indicate that their child is at risk of harm online
- Seek help and support from the school, or other appropriate agencies, if they or their child encounters online problems or concerns

Information system security:

The school ICT systems, capacity and security will be reviewed regularly by the ICT department. Virus protection will be updated regularly and security strategies will be in-line with the Local Authority. The ICT department will monitor internet use of all staff and pupils on a regular basis.

Passwords:

- All users will be informed not to share passwords or information with others and not to login as another user at any time
- Staff must always keep their password private and must not share it with others or leave it where others can find it. Pupils accounts on the server are not password protected
- All members of staff will have their own unique username and private passwords to access school systems. Members of staff are responsible for keeping their password private.
- We require staff to use STRONG passwords for access into our system.
- We require staff and pupils to change their passwords every term and should be significantly different to the previous password

Local Area Network (LAN) security issues include:

Users must act reasonably — e.g. the downloading of large files during the working day will affect the service that others receive.

- Users must take responsibility for their network use. For KCC staff, flouting electronic use policy is regarded as a reason for dismissal.
- Workstations should be secured against user mistakes and deliberate actions.
- Servers must be located securely and physical access restricted.
- Virus protection for the whole network must be installed and current.
- The server operating system must be secured and kept up to date.
- Access by wireless devices must be proactively managed and secured with a minimum of WPA2 encryption.

Wide Area Network (WAN) security issues include:

- HPSN2 is managed to prevent unauthorised access between schools.
- Decisions on WAN security are made on a partnership between schools and HCC.

Managing Filtering and Monitoring

No filtering or monitoring solution can offer the school 100% protection from exposure to inappropriate or illegal content so it is equally important that we demonstrate that we have taken all other reasonable precautions to safeguard children and staff.

Such methods include:

- Appropriate supervision
- Signing Acceptable Use Policy (staff, pupils, parents / carers)
- A robust and embedded online safety curriculum and appropriate up to date staff training
- The school will work with the Local Authority to ensure systems to protect pupils are reviewed and improved. If staff discover an unsuitable site it must be reported the Head Teacher and the ICT Coordinator
- It is the responsibility of the ICT department to ensure regular checks are made to ensure that filtering methods selected are appropriate, effective and reasonable. Class teachers are responsible for ensuring suitable teaching and learning within their classroom is taking place to ensure that pupils are using the internet safely and appropriately
- It is important to recognise that even with up to date security systems, filtering and monitoring, children or staff can potentially bypass them either via using proxy sites or by using their own devices
- Appropriate supervision, policy and procedures and up to date education and training are essential
- A reliance on filtering and monitoring alone to safeguarding children online could lead to a feeling of complacency which may put children and adults at risk of significant harm

The Senior Leadership Team and all staff responsible for teaching and learning should note that technologies such as mobile phones, iPads, and 'tablets' with wireless internet access can bypass school filtering systems and present a new route to undesirable material and communications.

Staying safe when using Online Communication

Email

- Personal email accounts should not be used for professional emails amongst colleagues, parents / carers and external agencies / professionals
- School email should be used for ALL communications in a professional context
- School emails are not private and con be monitored

- Professionals must ensure that their use of email at work always compiles with data protection legislation and confidential or personal data must not be sent electronically via email unless it is encrypted
- Staff should be appropriately trained and should ensure members of staff use appropriately secure email systems to share any sensitive or personal information
- Pupils are not given their own email accounts on the school system, where appropriate pupils will access emails via Purple Mash with its use monitored at all times by class staff
- Email communication must not reveal a pupil's personal details or those of others and pupils should not arrange to meet anyone – the risk of sharing data via school email should be considered
- Emails sent to an external organisation should be carefully written and authorised prior to sending in the same way as a letter written on school headed paper
- Emails sent from staff should be regarded as professional communication at all times
- The forwarding of chain mail is not permitted
- It is the responsibility of the user to ensure their password is not disclosed at any time

Content on the school website

- Contact information on the school website is the school address, admin email and telephone number. Staff and pupils' personal information will not be published on the school website
- The Executive Head Teacher, and Head of Schools will take overall responsibility and ensure that content is accurate and appropriate
- Any information published on the school website should be considered as professional
- Any information published on the school website should be checked prior to publishing

Pupils' images and work

- Photographs that include pupils will be carefully selected
- Pupils' full names will not be used anywhere on the website, particularly in association with photographs
- Written permission from parents and carers for the use of photographs on the website is requested as part of the annual data collection process. Any pupils without permission will not appear on the school website
- Any images posted on the school website should only be posted in consideration of other safeguarding and data protection policies

Classroom use of the Internet

Staff must be aware that:

- No search engine or filtering tool is ever completely safe, and appropriate supervision, use of safe search tools, pre-checks of search terms, age appropriate education for pupils and robust classroom management MUST be in place
- There is still always a risk that children will be exposed to inappropriate content

- The quality of the information on the Internet is variable
- Any devices children may bring to school should be stored in a locked cupboard until the end of the day
- ALL pupils MUST be supervised when using any device that is connected to the Internet. It is the responsibility of the classroom staff to ensure that pupils are supervised at all times
- All pupils and staff should be provided with Internet access to support educational outcomes
- If there are any concerns about the well-being of a child, the child's Internet access could be removed in alignment with the school's Behaviour Policy
- Parents should be involved in understanding the Home / School agreements

Social Media and Personal Publishing – See also Social Media Policy

There are benefits for communication, engagement, collaboration and learning via the Internet and social media, however alongside this there are risks associated with users including staff, pupils and the wider community

- The school will block / filter access to social networking sites such as Facebook and Twitter using Hampshire County Council's filtering software – many of these sites are at risk of being explosed to a great deal of advertising and could provide access to inappropriate content
- Pupils will be advised to never give out personal details of any kind which may identify them or their location
- Pupils and parents are advised that the use of social network spaces outside school brings a range of dangers to our pupils

Staff use of Social Networking sites (e.g. Facebook, Twitter, Snapchat, MSN messenger)

These rules are put in place to protect staff and pupils

- Staff should use the highest privacy settings when social networking
- Staff must NEVER become 'friends' with pupils of Heathfield School. SLT or the ICT coordinator should be made aware if a pupil makes a friend request to a member of staff
- Staff should NOT become 'friends' with parents or carers of pupils of Heathfield School

  It is important for staff to promote professional relationships with our pupils and their families and to maintain a boundary between their professional and personal lives

  Parents working in the school or for staff who have family members attending the school their priority should always be with the child and befriending school staff should be done so with caution
- Staff can become friends with other staff members
- DO NOT discuss under any circumstances the school, your colleagues, parents or pupils. Remember that things you say online can be taken and shared, sometimes out of context, with

others including employers, colleagues, parents and other children

- Remember that anything posted online can often be seen by "friends of friends" so your intended audience can widen to others
- Comments and images posted on social networking sites are on the internet forever – even if you have deleted them from your account. If the occasion arose, these could be traced and evidenced
- It is your responsibility to understand and use the available privacy settings N.B. There are not privacy settings that truly protect your privacy
- Do NOT post photographs taken in school
- Do NOT post any photographs taken of school staff unless you have their individual permission
- We ask you to consider the content of your posts and the effect they may have on the school, with particular emphasis to posts regarding illness or absence

"Friends" Facebook Group – It is the responsibility of each member of the group to consider what they share in this group. Whilst this is a closed group it is crucial that content shared amongst its members must take into account its audience as anything shared online can be taken and shared, sometimes out of context with others including employers, colleagues, parents and other children. DO NOT discuss under any circumstances the school, your colleagues, parents or pupils.
The purpose of "Friends" is for social use amongst colleagues. Work based discussions should occur via the school email network.

Please note that any misuse of Social Media Networking Sites that brings the school into disrepute or by not following the school's safety policy will lead to further disciplinary action

Pupils' use of social media
The school has a responsibility to ensure that pupils in the school have been provided with appropriate education around the safe use of the Internet and social media – this is part of the Computing Curriculum, and should be part of the PSHE curriculum

- Many sites have a restriction age of 13. It is not illegal for pupils under this age to access these sits, however it is not recommended because of the risk of them being targeted with unsuitable advertisements and content
- If pupils are using social media sites inappropriate (such as cyberbullying, posting personal information / material, adding strangers as friends, etc) or there are other safeguarding concerns due to their vulnerabilities, etc, then the school should respond to the concern in line with existing policies (e.g. Safeguarding Policy, Behaviour Policy)
- If a child is at risk of significant harm then the DSL must be informed and the existing child protection procedures should be followed

The use of personal devices and mobile phones

- Personal devices and mobile phones will not be used during lessons, meetings or training. The sending of abusive or inappropriate messages is forbidden either by text, Bluetooth or any other means
- Personal mobile phones MUST NOT be used to take photographs of pupils
- Staff will use a school phone where contact with parents or the school may be required (e.g. on bus trips)
- If a pupil brings a mobile phone into school it must be given to an adult and kept secure until home time. The use of mobile phones by pupils is forbidden
- On trips it may be deemed appropriate for staff to use their mobile phones in case of an emergency to contact the school, emergency services or parents. School mobile phones should be used as a first port of call to protect the personal contact information of the staff member. In the event that a staff member is required to use their phone, they should consider that their phone is used only to make contact
- Staff are discouraged from using their personal devices for recording images and video. The school issues cameras and school devices for this purpose
- Staff are not permitted to use their mobile phones during teaching sessions unless permission has been given by a member of the Senior Leadership team in emergency circumstances
- Any allegations against a member of staff involving personal use of a mobile phone or device will be responded to following the school allegations management policy
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence then the police will be contacted
- If a member of staff breaches the school policy then disciplinary action will be taken
- Staff will ensure that any content bought on site via mobile phones and personal devices are compatible with their professional role and expectations

Games machines

- Games machines brought into school by a pupils must be given to an adult and kept secure until home time. The use of games machines brought in from home by pupils is forbidden
- Pupils may access the Xbox or Nintendo Wii when supervised by an adult. These do not have internet access

Sexting

- "Sexting" can be defined as images or videos generated by children under the age of 18 that are of a sexual nature or are considered to be indecent. Children typically refer to images as "selfies" and may decide to send such pictures or videos for many reasons

- If anyone is found to be in possession of an indecent image of a minor this is an offence under the Protection of Children Act 1978 and Section 160 of the Criminal Justice Act 1988 – under this legislation if it a crime to take an indecent photograph or allow an indecent photograph to be taken, make an indecent photograph (including downloading or opening an image sent via email); distribute or show an indecent image, advertise indecent images and possess an indecent image or possess an indecent image with the intention of distribution. This applies even if the images are sent or shared by someone under the age of 18 with consent. "Sexts" may be viewed as police evidence and it is essential that schools secure devices and seek advice immediately when dealing with concerns
- Younger children may take or share indecent images or videos out of curiosity or naivety and for older children, indecent images may be taken or shared as a response to peer pressure, cyberbullying, sexual exploration, impulsive behaviour or even exploitation due to blackmail from a friend, partner, or other on or offline contact
- There can also be emotional and reputation damage that can come from having intimate photos forwarded to others or shared online including isolation, bullying, low self-esteem, loss of control, creating of a negative "digital footprint" or online reputation, harassment, mental health difficulties, self-harm, suicide and increased risk of child sexual exploitation
- NEVER send explicit messages or images to a colleague, parent / carer or pupil.
- If you are made aware of a pupil having received an explicit message or image this MUST be reported immediately to the Designated Child Protection Officer. Any concerns or incidents involving "sexting" should be dealt with carefully and support should be offered to all parties involved whilst abiding by the law and without compromising police investigations

Grooming

Online child sexual abuse within this policy context is specifically defined as when children are sexually abused or exploited via the use of technology and the Internet.

- This is referred to as "online grooming": This is used to describe how people who want to sexually harm children and young people get close to them. Online grooming may occur when people pretend to be a friend to someone, although there is no set time frame for this
- At Heathfield School we have a set of E-Safety Rules in place to protect our pupils from giving out personal information about them. Pupils where it is deemed appropriate will access the school's E-Safety Scheme of Work and will be taught the 5 key "Childnet SMART Rules".
- If you have any concerns regarding a pupil being groomed then it is your responsibility to report this to the Designated Child Protection Officer immediately.

Radicalisation and Extremism Online

Heathfield School is mindful of the specific responsibilities and requirements placed upon us under the Prevent Duty:

https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty

From 1st July 2015, specified authorities, including schools are subject to a duty under Section 26 of the Counter-Terrorism and Security Act 2015 in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism".
This duty is known as the Prevent Duty – the statutory Prevent guidance summarises the requirements on schools as undertaking risk assessment, working in partnership, staff training and IT policies.

Heathfield School assesses the risk of pupils being drawn into terrorism, such as support for extremism views that are part of terrorist ideology and a range of extremist views including the far right.

- Procedures are detailed in the Safeguarding Policy, and this policy plays an important role as it highlights the action the school will take to ensure that pupils are safe from terrorist and extremist material when accessing the Internet in school.
- Filtering and monitoring systems are in place, however staff should be mindful to act in accordance with the law. It should also be noted that radicalisation and extremist views can be shared and accessed on a variety of platforms, including user generated or social media sites such as Facebook and YouTube.
- Therefore it is crucial that all pupils are carefully supervised when using the Internet in school.
- As part of the PSHE curriculum, discussions will take place at an appropriate time and with resources that are available to ensure that safeguarding measures are in place to ensure that the range of risks including radicalisation and extremism, alongside grooming and sexual exploitation are in place
- Any device that does not require a login or password to access the Internet should be monitored closely at all times by staff and kept in a locked cupboard when not in use.
- All staff should always be aware that simply relying on filtering to prevent radicalisation will not be sufficient as children are likely to have access to a range of devices at home which may not be filtered or monitored. Education around safe use is therefore essential.
- As with all safeguarding risks, all members of staff should be alert to changes in the pupils' behaviour which may indicate that they may be at risk or in need of specific help or protection
- All members of staff should receive appropriate training to enable them to explore their responsibilities with regards to prevent for safeguarding pupils and adults within the school community

The school will take all reasonable precautions to ensure that children are safe from terrorist and extremist material when accessing the Internet in school and that suitable filtering is in place which takes into account the needs of pupils

Cyberbullying

Online or cyberbullying can be defined as the use of Information Communication Technology, particularly mobile phones and the Internet to deliberately hurt or upset someone

- Cyberbullying is becoming increasingly prevalent with the rapid advances and use of modern technology
- Mobile, Internet and wireless technologies have increased the pace of communication and brought significant benefits to users worldwide
- However, their popularity provides increasing opportunity for misuse through 'cyberbullying', with worrying consequences
- It is crucial that children, young people and adults use their devices and the Internet safely and positively and they are aware of the consequences of misuse
- When children and adults are the target of bullying via mobile phones, gaming or the Internet (including Social Media sites), they can often feel very alone, particularly if those around them do not understand online bullying and its effects
- Cyberbullying may not always be intentional, and repeated in the same way that traditional bullying is, however a previously safe and enjoyable activity can become threatening, harmful and a source of anxiety
- People may not feel that they are bullying online, it is important that all incidents of online abuse are addressed as early as possible to prevent escalation
- Education staff, parents and parents / carers have to be constantly vigilant and work together to prevent this and tackle it wherever it appears
- Cyberbullying is a method of bullying and should be viewed and treated the same as "real world" bullying and can happen to any member of the school community
- Staff must be aware that abuse can be perpetuated by children themselves including cyberbullying and staff must be aware of concerning behaviour and appropriate safeguarding responses
- Promoting a culture of confident users will support innovation and safety, young people, staff and parents / carers need to understand how to respond and combat cyberbullying

There are a number of statutory obligations with regard to behaviour which establish clear responsibilities to respond to bullying. In particular Section 89 of the Education and Inspections Act 2006:

- Every school must have measures to encourage good behaviour and prevent all forms of bullying amongst pupils. These measures should be part of the school's Behaviour Policy which must be communicated to all pupils, school staff and parents
- Gives Head Teachers' the ability to ensure that pupils behave when they are not on school premises or under the lawful control of school staff

When online bullying takes place outside school is reported then it must be investigated and acted on appropriately by Heathfield School

Under the Children Act 1989, a bullying incident should be addressed as a child protection concern when there is 'reasonable cause to suspect that a child is suffering, or is likely to suffer, significant harm'

Online hate

Hate crimes are any crimes targeted at a person because of hostility or prejudice towards that person's:

- Disability
- Race or ethnicity
- Religion or belief
- Sexual orientation
- Transgender identity

School's must ensure that they respond appropriately regarding online hate and discrimination and support members of the community who may be targeted online

Use of cameras

At Heathfield School we often use cameras and Android Tablets to take photographs of the pupils' work and to capture their learning.
We have a responsibility to ensure that any device used is issued by the school and is kept in a locked cupboard over night
School staff have a responsibility to clear any images from the camera within one week and store images on the school's secure server which is password protected

Authorising internet access

- All staff, including those not directly employed by us but working in school must read and sign the 'Staff and Volunteer Acceptable Use Policy' (see attached Appendix 1)

Assessing Risks

- The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the international scale and linked nature of internet content, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school not Hampshire County Council can accept liability for the material access or any consequence of internet access
- The school will audit ICT provision to establish if the e-safety policy is adequate and that its implementation is effective

Handling E-Safety complaints

- Any complaints of internet misuse will be dealt with by the Head Teacher
- Complaints of a child protection nature must be dealt with in accordance with the school child protection procedures

Introducing E-Safety to pupils

- E-safety rules, in Communicate in Print, will be posted in classrooms and discussed with pupils as part of their learning, where appropriate

- Pupils will be informed that network and internet use if monitored
- E-Safety training will be embedded within ICT teaching and learning and as part of the Personal, Social Education curriculum (PDL)
- Parents will be encouraged to support this at home with their child

Staff and the E-Safety Policy

- All staff will be made aware of the School E-Safety Policy, Social Media Policy, Safeguarding Policy and their importance explained
- A copy will be available in the staff room
- Staff will be made aware that internet traffic will be monitored and traced to an individual user. Discretion and professional conduct is essential
- Online safety education should be part of the annual safeguarding training that statutorily takes place in schools

Parents / Carers Support

- Parents' attention will be drawn to the School E-Safety Policy, Social Media Policy, Safeguarding Policy in newsletters, the school website and parents will be asked to sign an 'Acceptable Use Policy' for pupils at the beginning of each school year
- Technology is a tool that is commonly used in the home environment. It is therefore important that parents and carers are provided with the opportunity to hear about the benefits and risks of technology and how these can be managed

Awareness-raising with families should focus on:

- The range of different ways children and young people use and access technology e.g. mobile phones, games consoles, tablets and apps etc. not just laptops and computers.
- The many positive uses of technology as otherwise online safety can easily become frightening and scaremongering so be aware that the vast majority of interactions and experiences on the internet are positive!
- The importance of developing risk awareness and risk management by children and young people (according to their age and ability) and resources parents/carers can use to help discuss online safety

Further Reading

- https://www.gov.uk/government/publications/keeping-children-safe-in-education--2
- Further information from Hampshire Parents and Carers, Practitioners and Pupils can be found online

http://www3.hants.gov.uk/childrens-services/schoolsandcolleges/esafety.htm

Policy by: Hayley Sae Kang (Computing Co-Ordinator)

Date: February 2016; Reviewed: March 2017; December 2017

To be reviewed: February 2018