E-Safety Policy

Date Published	**December 2020**
Version	**1**
Approved Date	**March 2022**
Review Cycle	**1 Year**
Review Date	**March 2023**

An academy within:

Multi Academy Trust

Learning together to be the best we can be

1. Scope

1.1. This policy applies to all members of the school (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school digital technology systems, both in and out of the school.

1.2. The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other E-Safety incidents covered by this policy, which may take place outside of the school, but is linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

2. Roles & Responsibilities

2.1. **Nexus Multi Academy Trust**

2.1.1. Nexus MAT Board of Directors are responsible for the approval of school policies, and local governing bodies have delegated responsibility for reviewing the effectiveness of the policy. This will be carried out by the local governors receiving regular information about E-Safety incidents within monitoring reports. The local governing body has a named link governor for safeguarding, who will focus on E-Safety as part of that wider remit.

2.2. **The School Senior Leadership Team**

2.2.1. The Headteacher has a duty of care for ensuring the safety (including E-Safety) of members of the school community, though the day to day responsibility for E-Safety will be delegated to the E-Safety Lead.

2.2.2. The Headteacher and (at least) another member of the Senior Leadership Team 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 – included in a later section – "Responding to incidents of misuse")

2.2.3. The Headteacher & Senior Leaders are responsible for ensuring that the E-Safety Lead and other relevant staff receive suitable training to enable them to carry out their E-Safety roles and to train other colleagues, as relevant.

2.2.4. The Headteacher & Senior Leaders 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. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

2.2.5. The Senior Leadership Team will receive regular monitoring reports from the E-Safety Lead.

2.3. E-Safety Lead

- leads the E-Safety Group;
- 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 taking place;
- provides training and advice for staff;
- liaises with relevant bodies;
- liaises with school technical staff;
- receives reports of E-Safety incidents and creates a log of incidents to inform future E-Safety developments;
- meets regularly with E-Safety Governor to discuss current issues, review incident logs and filtering / change control logs;
- attends relevant meetings;
- reports regularly to Senior Leadership Team.

2.4. Network Manager / Technical staff

2.4.1. The Network Manager is responsible for ensuring:

- that the school's technical infrastructure is secure and is not open to misuse or malicious attack

- that the school meets required E-Safety technical requirements and any E-Safety Policy / Guidance that may apply.
- that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- the filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- that they keep 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
- that the use of the network / internet / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher/ Senior Leader; E-Safety Lead for investigation / action / sanction
- that monitoring software / systems are implemented and updated as agreed in school policies
- Makes clear that staff accessing NHS systems do so in accordance with any corporate Sheffield Children's Hospital policies (see policy in appendices).

2.5. **Teaching and Support Staff**

2.5.1. 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 Staff Acceptable Use Policy/ Agreement (AUP)
- they report any suspected misuse or problem to the Headteacher /Senior Leader; E-Safety Lead for investigation / action / sanction
- all digital communications with students / pupils / parents / carers should be on a professional level and only carried out using official school systems
- E-Safety issues are embedded in all aspects of the curriculum and other activities
- students / pupils understand and follow the E-Safety Policy and acceptable use policies
- students / pupils have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- they monitor the use of digital technologies, mobile devices, cameras etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- in lessons where internet use is pre-planned students / 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

2.6. **Designated Safeguarding Lead**

2.6.1. Should be trained in E-Safety issues and be aware of the potential for serious child protection / safeguarding 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
- online-bullying

2.7. **E-Safety Group**

2.8. The E-Safety Group provides a consultative group that has representation from the school community, with responsibility for issues regarding E-Safety and the monitoring the E-Safety Policy including the impact of initiatives. This group is part of the safeguarding group. The group will also be responsible for regular reporting to the Local Governing Body.

2.9. Members of the E-Safety Group will assist the E-Safety Lead with

- the production / review / monitoring of the school E-Safety Policy / documents;
- the production / review / monitoring of the school filtering policy and requests for filtering changes;
- mapping and reviewing the E-Safety / digital literacy curricular provision – ensuring relevance, breadth and progression;
- monitoring network / internet / incident logs;
- consulting stakeholders – including parents / carers and the students / pupils about the E-Safety provision;
- monitoring improvement actions identified through use of the 360-degree safe self-review tool.

2.10. Students / Pupils

- are responsible for using the school digital technology systems in accordance with the Student / Pupil Acceptable Use Agreement;
- have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-bullying;
- should understand the importance of adopting good E-Safety practice when using digital technologies out of school and realise that the school's E-Safety Policy covers their actions out of school, if related to their membership of the school.

2.11. Parents / Carers

2.12. Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The school will take every opportunity to help parents understand these issues through parents' evenings, letters, website and information about national / local E-Safety campaigns / literature. Parents and carers will be encouraged to support the school in promoting good E-Safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at school events;
- access to parents' sections of the website and on-line student / pupil records;
- children's personal devices in the school (where this is allowed).

2.13. Community Users

2.13.1. Community Users who access school systems / website as part of the wider school provision will be expected to sign a Community User AUA before being provided with access to school systems.

3. Education Policy Statements

3.1. Student & Pupils

3.1.1. Whilst regulation and technical solutions are very important, their use must be balanced by educating students / pupils to take a responsible approach. The education of students / pupils in E-Safety / digital literacy 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.

3.1.2. E-Safety should be a focus in all areas of the curriculum and staff should reinforce E-Safety messages across the curriculum. The E-Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned E-Safety curriculum should be provided as part of PHSE lessons and should be regularly revisited
- Key E-Safety messages should be reinforced as part of a planned programme of tutorial / pastoral activities
- Students / pupils should be taught in all lessons to be critically aware of the materials / content they access on-line and be guided to validate the accuracy of information.
- Students / pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students / pupils should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making.
- Students / pupils should be helped to understand the need for the student / pupil Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices in lessons where internet use is pre-planned, it is best practice that students / 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 students / pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

3.2. Parents / Carers

3.2.1. 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 / regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, web site,
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. swgfl.org.uk www.saferinternet.org.uk/ http://www.childnet.com/parents-and-carers (see appendix for further links / resources)

3.3. The Wider Community

3.3.1. The school will provide opportunities for local community groups / members of the community to gain from the school's E-Safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and E-Safety
- E-Safety messages targeted towards grandparents and other relatives as well as parents.
- The school website will provide E-Safety information for the wider community.

3.4. Staff / Volunteers

3.4.1. 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. This will be regularly updated and reinforced. An audit of the E-Safety training needs of all staff will be carried out regularly.
- 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 Agreements.
- It is expected that some staff will identify E-Safety as a training need within the performance management process.
- The E-Safety Lead (or other nominated person) will receive regular updates through attendance at external training events (e.g. from CEOP /other relevant organisations) and by reviewing guidance documents released by relevant organisations.
- This E-Safety Policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.
- The E-Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

3.5. Local Governors

3.5.1. Local governors should take part in E-Safety training / awareness sessions, with particular importance for those who are link governors. This may be offered in a number of ways:

3.5.2. Attendance at training provided by relevant organisation;

3.5.3. Participation in school training / information sessions for staff or parents.

4. Technical – infrastructure/equipment, filtering and monitoring

4.1. The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people named in the above sections will be effective in carrying out their E-Safety responsibilities:

4.1.1. School technical systems will be managed in ways that ensure that the school meets recommended technical requirements;

4.1.2. There will be regular reviews and audits of the safety and security of school technical systems;

4.1.3. Servers, wireless systems and cabling must be securely located and physical access restricted;

4.1.4. All users will have clearly defined access rights to school technical systems and devices;

4.1.5. Where appropriate, and dependent upon pupils' cognitive understanding, ~~All~~ users (at KS2 and above) will be provided with a username and secure password by the school engineer who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password;

4.1.6. The "master / administrator" passwords for the school ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher or other nominated senior leader and kept in a secure place (e.g. school safe);

4.1.7. The school engineer responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations;

4.1.8. Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes;

4.1.9. Internet filtering / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet;

4.1.10. The school has provided enhanced / differentiated user-level filtering;

4.1.11. School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement;

4.1.12. An appropriate system is in place for users to report any actual / potential technical incident / security breach to the relevant person, as agreed);

4.1.13. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual workstations are protected by up to date virus software;

4.1.14. An agreed policy is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school systems;

4.1.15. An agreed policy is in place regarding the extent of personal use that users (staff / students / pupil's / community users) and their family members are allowed on school devices that may be used out of school;

4.1.16. Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.

5. Mobile Technologies (including BYOD/BYOT)

5.1. Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, notebook / laptop or other technology that usually has the capability of utilising the school's wireless network. The device then has access to the wider internet which may include the school's learning platform and other cloud based services such as email and data storage.

5.2. All users should understand that the primary purpose of the use mobile / personal devices in a school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school polices including but not limited to the Safeguarding Policy, Behaviour Policy, Bullying Policy, Acceptable Use Policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's E-Safety education programme.

5.3. The Trust Acceptable Use Agreements for staff, pupils/students and parents / carers will give consideration to the use of mobile technologies.

5.4. The school allows:

	School Devices			Personal Devices		
	School owned for single user	**School owned for multiple users**	**Authorised device[1]**	**Student owned**	**Staff owned**	**Visitor owned**
Allowed in school	*Yes*	*Yes*	*Yes*	*Yes – To be handed in at the beginning of the day*	*Yes*	*Yes*
Full network access	*Yes*	*Yes*	*Yes*	*No*	*No*	*No*
Internet only				*No*	*No*	*No*
No network access				*No*	*No*	*No*

6. Use of digital and video images

6.1. The development of digital imaging technologies has created significant benefits to learning, allowing staff and students / pupils instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students / pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

[1] Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

6.1.1. When using digital images, staff should inform and educate students / 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.

6.1.2. Written permission from parents or carers will be obtained before photographs of students / pupils are published on the school website / social media / local press

6.1.3. In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students / pupils in the digital / video images.

6.1.4. Staff and volunteers are allowed to take digital / 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 taken on school equipment; the personal equipment of staff should not be used for such purposes.

6.1.5. Care should be taken when taking digital / video images that students / pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute.

6.1.6. Students / pupils must not take, use, share, publish or distribute images of others without their permission

6.1.7. Photographs published on the website, or elsewhere that include students / pupils will be selected carefully and will comply with good practice guidance on the use of such images.

6.1.8. Students' / Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.

6.1.9. Student's / Pupil's work can only be published with the permission of the student / pupil and parents or carers.

7. Data Protection

7.1. The school must comply with the Trust's data protection requirements, which are published in the Nexus MAT Information Governance Policy.

8. Communications

8.1. A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the school currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults			Students / Pupils				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	Y						Y	
Use of mobile phones in lessons		Y					Y	
Use of mobile phones in social time	Y			Y				
Taking photos on mobile phones / cameras		Y					Y	
Use of other mobile devices e.g. tablets, gaming devices		Y		Y				
Use of personal email addresses in school , or on school network		Y		Y				
Use of school email for personal emails		Y					Y	
Use of messaging apps			Y	Y				
Use of social media			Y	Y				
Use of blogs			Y	Y				

8.2. When using communication technologies, the school considers the following as good practice:

8.2.1. The official school email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students / pupils should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access).

8.2.2. Users must immediately report, to the nominated person – in accordance with the school policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

8.2.3. Any digital communication between staff and students / pupils or parents / carers (email, social media, chat, blogs, 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 social media must not be used for these communications.

8.2.4. Whole class / group email addresses may be used at KS1, while students / pupils at KS2 and above will be provided with individual school email addresses for educational use where appropriate and depending on pupil cognitive understanding.

8.2.5. Students / pupils should be taught about E-Safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

8.2.6. Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.

9. Social Media - Protecting Professional Identity

9.1. All schools have a duty of care to provide a safe learning environment for pupils and staff. Schools and local authorities could be held responsible, indirectly for acts of their employees in the course of their employment. Staff members who harass, engage in online bullying, discriminate on the grounds of sex, race or disability or who defame a third party may render the school or local authority liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

9.2. The school provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and the school through:

9.2.1. Ensuring that personal information is not published;
9.2.2. Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues;
9.2.3. Clear reporting guidance, including responsibilities, procedures and sanctions;
9.2.4. Risk assessment, including legal risk.

9.3. School staff should ensure that:

9.3.1. No reference should be made in social media to students / pupils, parents / carers or school staff;
9.3.2. They do not engage in online discussion on personal matters relating to members of the school community;
9.3.3. Personal opinions should not be attributed to the school;
9.3.4. Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

9.4. When official school social media accounts are established there should be:

9.4.1. A process for approval by senior leaders;
9.4.2. Clear processes for the administration and monitoring of these accounts – involving at least two members of staff;
9.4.3. A code of behaviour for users of the accounts, including;
9.4.4. Systems for reporting and dealing with abuse and misuse;
9.4.5. Understanding of how incidents may be dealt with under school disciplinary procedures.

9.5. Personal Use:

9.5.1. Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with the school or impacts on the school, it must be made clear that the member of staff is not communicating on behalf of the school; with an appropriate disclaimer. Such personal communications are within the scope of this policy;

9.5.2. Personal communications which do not refer to or impact upon the school are outside the scope of this policy;

9.5.3. Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken;

9.5.4. The school permits reasonable and appropriate access to private social media sites.

9.6. Monitoring of Public Social Media:

9.6.1. As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the school

9.6.2. The school should effectively respond to social media comments made by others according to a defined policy or process

9.6.3. The school's use of social media for professional purposes will be checked regularly by the senior risk officer and E-Safety Group to ensure compliance with the school policies.

10. Dealing with unsuitable / inappropriate activities

10.1. Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in a school /academy context, either because of the age of the users or the nature of those activities.

10.2. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in / or outside the school when using school equipment or systems. The school policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	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				X	
Using school systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					X	
Infringing copyright					X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)					X	
Creating or propagating computer viruses or other harmful files					X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)					X	

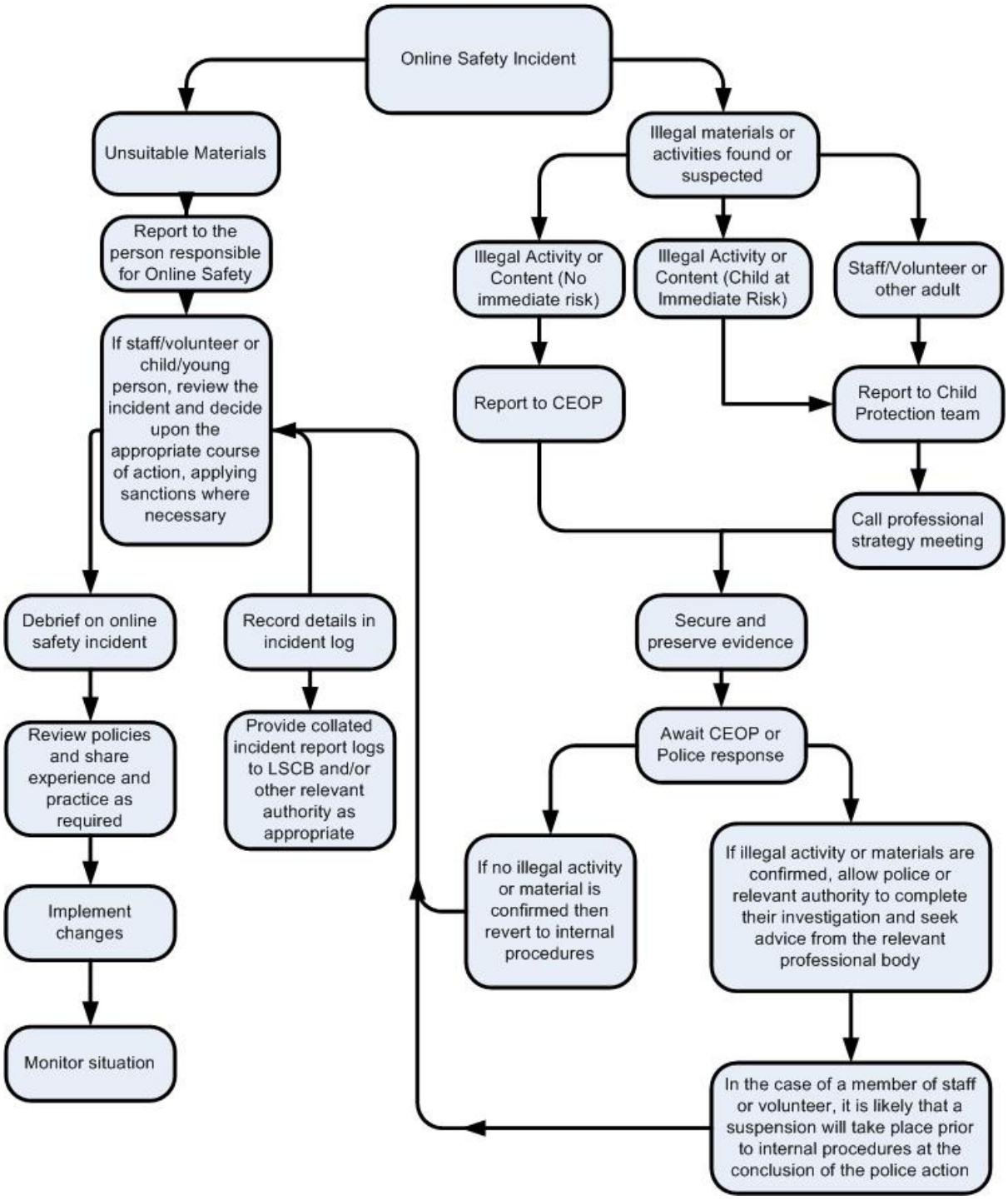
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps			X		
Use of video broadcasting e.g. YouTube		x			

11. Responding to incidents of misuse

11.1. This guidance is intended for use when staff need 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 involve illegal or inappropriate activities (see "User Actions" above).

12. Illegal Incidents

12.1. If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to E-Safety incidents and report immediately to the police.


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

13. Other Incidents

13.1. It is hoped that all members of the school community will be responsible users of digital technologies, who understand and follow school policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

13.2. In the event of suspicion, all steps in this procedure should be followed:

13.2.1. Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.

13.2.2. 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.

13.2.3. 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).

13.3. 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).

13.4. 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:

13.4.1. Internal response or discipline procedures

13.4.2. Involvement by Local Authority / Academy Group or national / local organisation (as relevant).

13.4.3. Police involvement and/or action

13.5. 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:

13.5.1. incidents of 'grooming' behaviour
13.5.2. the sending of obscene materials to a child
13.5.3. adult material which potentially breaches the Obscene Publications Act
13.5.4. criminally racist material
13.5.5. promotion of terrorism or extremism
13.5.6. other criminal conduct, activity or materials

13.6. Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

14. School Actions & Sanctions

14.1. 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 follows:

Actions / Sanctions

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

Actions / Sanctions

Students / Pupils Incidents	Refer to class teacher / tutor	Refer to Head of Department / Year / other	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	X	X
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	X	X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X	X	X	X	X
Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X	X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act	X	X	X	X	X	X	X	X	X

	Actions / Sanctions							
Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to HR	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Warning	Suspension	Disciplinary action
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		X	X	X				
Inappropriate personal use of the internet / social media / personal email	X	X			X	X		
Unauthorised downloading or uploading of files	X	X			X	X		
Allowing others to access school network by sharing username and passwords or attempting to access or accessing the school network, using another person's account	X	X	X		X	X	X	
Careless use of personal data e.g. holding or transferring data in an insecure manner	X	X	X		X	X		
Deliberate actions to breach data protection or network security rules	X	X	X	X	X	X	X	X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X	X	X
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / pupils	X	X	X		X	X		
Actions which could compromise the staff member's professional standing	X	X	X		X	X	X	
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school	X	X	X		X	X	X	
Using proxy sites or other means to subvert the school's / academy's filtering system	X	X	X		X	X	X	
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X		X			

Deliberately accessing or trying to access offensive or pornographic material	X	X	X	X	X	X	X	X
Breaching copyright or licensing regulations	X	X	X		X	X	X	
Continued infringements of the above, following previous warnings or sanctions	X	X	X	X	X	X	X	X

Appendices

Appendix A - Student / Pupil Acceptable Use Agreement

Appendix B - Student / Pupil Acceptable Use Agreement Form

Appendix C - Student / Pupil Acceptable Use Policy Agreement for younger pupils

Appendix D - Parent / Carer Acceptable Use Agreement Template

Appendix E - Staff (and Volunteer) Acceptable Use Policy Agreement

Appendix F - Acceptable Use Agreement for Community Users

Appendix G - Glossary of Terms

Appendix H - Sheffield Children's Hospital Acceptable Use Agreement

Student / Pupil Acceptable Use Agreement

School Policy

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

This Acceptable Use Agreement is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

Acceptable Use Policy Agreement

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

For my own personal safety:

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

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

- I understand that the *school* systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the *school* systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

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

- I will only use my own personal devices (mobile phones / USB devices etc.) in school if I have permission
- I understand that, if I do use my own devices in the *school*, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any school device, nor will I try to alter computer settings.

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

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

Appendix A - Student / Pupil Acceptable Uuse Agreement

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

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

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

Appendix B
Student/Pupil Acceptable Use Agreement Form

Student / Pupil Acceptable Use Agreement Form

This form relates to the *student / pupil* Acceptable Use Agreement; to which it is attached.

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

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

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

Name of Student / Pupil: .....

Group / Class: .....

Signed: .....

Date: .....

Appendix C
Student/Pupil Acceptable Use Agreement Form for younger pupils

Student / Pupil Acceptable Use Policy Agreement for younger pupils

This is how we stay safe when we use computers:

- I will ask a teacher or suitable adult if I want to use the computers / tablets
- I will only use activities that a teacher or suitable adult has told or allowed me to use
- I will take care of the computer and other equipment
- I will ask for help from a teacher or suitable adult if I am not sure what to do or if I think I have done something wrong
- I will tell a teacher or suitable adult if I see something that upsets me on the screen
- I know that if I break the rules I might not be allowed to use a computer / tablet

Signed (child): .....

Parent / Carer Acceptable Use Agreement Template

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

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of E-Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The school will try to ensure that *students / pupils* will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users. A copy of the *Student / Pupil* Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name: .....

Student / Pupil Name:... .....

As the parent / carer of the above *students / pupils*, 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 technology and the internet – both in and out of school.

I understand that the school has discussed the Acceptable Use Agreement with my son / daughter and that they have received, or will receive, E-Safety education to help them understand the importance of safe use of technology and the internet – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and 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 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.

Acceptable Use Policy
Accessed by school staff
Stored in pupil folder
Stored for the duration of time that the pupil is on roll + 1 month
Shredded when pupil has come off-roll

Signed: .....

Date: .....

Appendix A - Student / Pupil Acceptable Uuse Agreement

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. *Students / 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. Where an image is publically shared by any means, only your child's first name/initials will be used.

The school will comply with the Data Protection Act and request parent's / 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 the use of their names.

In accordance with guidance from the Information Commissioner's Office, parents / carers are welcome to take videos and digital images of their children at school events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other *students / pupils* in the digital / video images.

Parents / carers are requested to sign the permission form below to allow the school to take and use images of their children and for the parents / carers to agree.

This form (electronic or printed)	The images
This form will be accessed by authorised staff at Heatherwood School.	The images may be published. on Twitter, the school website or the local press,
This form will be stored as an electronic copy in the pupil file	The images will be accessed by authorised staff at Heatherwood School. .
This form will be stored for the period in which you are involved with Heatherwood School +1 month	The images will be stored as an electronic file in the secure staff area of the network

Appendix A - Student / Pupil Acceptable Uuse Agreement

This information will be deleted from the Electronic records.	The images will be stored for the period in which you are involved with Heatherwood School +1 month
	The images will be deleted from the server
	A request for deletion can be made to the Head Teacher

Digital / Video Images Permission Form

Parent / Carers Name:..... Student / Pupil Name:.....

As the parent / carer of the above student / pupil, I agree to the school taking digital / video images of my child / children.	Yes / No
I agree to these images being used:	
• to support learning activities.	Yes / No
• in publicity that reasonably celebrates success and promotes the work of the school.	Yes / No
Insert statements here that explicitly detail where images are published by the school	Yes / No
I agree that if I take digital or video images at, or of – school events which include images of children, other than my own, I will abide by these guidelines in my use of these images.	Yes / No

Signed: .....

Date: .....

Student / Pupil Acceptable Use Agreement

On the following pages we have copied, for the information of parents and carers, the Student / Pupil Acceptable Use Agreement.

Staff (and Volunteer) Acceptable Use Policy Agreement

School Policy

New technologies have become integral to the lives of children and young people in today's society, both within schools / academies and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe access to the internet and digital technologies at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.

The school will try to ensure that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for *students / pupils* learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology 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 school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, VLE etc.) out of school, and to the transfer of personal data (digital or paper based) out of school
- I understand that the school digital technology 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. (schools should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of school systems)

Appendix E
Staff (and Volunteer) Acceptable Use Policy Agreement

- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 / video 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) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / 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*:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using *school* equipment. I will also follow any additional rules set by the *school* about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will 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 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.

Appendix E
Staff (and Volunteer) Acceptable Use Policy Agreement

- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student / 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 school 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 the *school*:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises 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 include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name: .....

Signed: .....

Date: .....

Appendix F

Acceptable Use Agreement for Community Users

Acceptable Use Agreement for Community Users

This Acceptable Use Agreement is intended to ensure:

- that community users of school digital technologies will be responsible users and stay safe while using these systems and devices
- that school systems, devices and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that users are protected from potential risk in their use of these systems and devices

Acceptable Use Agreement

I understand that I must use school systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into the school:

- I understand that my use of school) systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into school for any activity that would be inappropriate in a school setting.
- 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 immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in the school on any personal website, social networking site or through any other means, unless I have permission from the school.
- I will not, without permission, make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a school device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- 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).

Appendix F

Acceptable Use Agreement for Community Users

- I understand that if I fail to comply with this Acceptable Use Agreement, the school has the right to remove my access to school systems / devices

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

This form will be accessed by authorised staff at Heatherwood School.
This form will be stored as an electronic copy in the pupil file
This form will be stored for the period in which you are involved with Heatherwood School +1 month
This information will be deleted from the Electronic records.

Name: ..... Signed: .....

Date: .....

Glossary of Terms

AUP / AUA	Acceptable Use Policy / Agreement – see templates earlier in this document
CEOP	Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.
CPD	Continuous Professional Development
FOSI	Family E-Safety Institute
ICO	Information Commissioners Office
ICT	Information and Communications Technology
ICTMark	Quality standard for schools provided by NAACE
INSET	In Service Education and Training
IP address	The label that identifies each computer to other computers using the IP (internet protocol)
ISP	Internet Service Provider
ISPA	Internet Service Providers' Association
IWF	Internet Watch Foundation
LA	Local Authority
LAN	Local Area Network
MIS	Management Information System
NEN	National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to schools across Britain.
Ofcom	Office of Communications (Independent communications sector regulator)
TUK	Think U Know – educational E-Safety programmes for schools, young people and parents.
WAP	Wireless Application Protocol
UKSIC	UK Safer Internet Centre – EU funded centre. Main partners are SWGfL, Childnet and Internet Watch Foundation.

Appendix G

Glossary of Terms