HODGE HILL GIRLS' SCHOOL

"Educating tomorrow's women today"

hyt\yŜ {I-ŦŜűè Policy

Document Information	
Role of individual completing review:	ICT Operations Manager
Approved by:	Curriculum & Pastoral
Date approved:	20/05/2024
Date of next review:	May 2025
Additional notes:	Removal of Appendix a1-a5 now in Student AUP

Hodge Hill Girls' School

Online Safety Policy

Contents

1 Aims

1.1 Hodge Hill Girls' School aims to:

- have robust processes and systems in place to ensure the online safety of pupils, staff, visitors and governors
- deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology
- establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

2 Legislation and Guidance

2.1 This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation.

2.2 It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given authorised staff stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils' electronic devices where they believe there is a 'good reason' to do so.

3 Scope of the Policy

3.1 This policy applies to all members of the school community (including staff, pupils, volunteers, parents / carers, visitors, community users, suppliers, contractors) who have access to and are users of school digital technology systems, both in and out of school, and to personal devices owned by adults and young people used in school.

3.2 This policy also applies to all members of the school community who represent the school (including staff, pupils, volunteers) whose technology or internet activity in or out of school could bring into disrepute the school's reputation or personal professionalism.

3.3 The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying, or other Online 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. In the case of both Acts, action can only be taken over issues covered by the published Behaviour Policy / Professional Learning Standards.

3.4 The school will deal with such incidents within this policy and associated Behaviour Policy, Professional Learning Standards and School Bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of school.

3.5 Some material available via the internet is unsuitable for school users. The school will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that unsuitable material will never appear on a school computer. Neither the school nor the Local Authority can accept responsibility for the material accessed, or any consequences of internet access.

4 Roles and Responsibilities

Online safety depends on the school, staff, governors, parents and the pupils themselves taking responsibility for their actions online. Staff have a particular responsibility to supervise pupils, plan access and be an appropriate role model.

4.1 The Governing body

4.1.1 The Governing body will monitor the effectiveness of this policy and hold the Headteacher to account for its implementation.

4.1.2 This will be carried out by the Governing body:

- reading and understanding this policy
- receiving regular information about online safety incidents and monitoring reports from the Designated Safeguarding Lead once per term at Governing body meetings.

4.2 Headteacher and Senior Leaders

4.2.1 The Headteacher is responsible for:

- ensuring the safety (including online safety) of members of the school community
- ensuring that staff understand this policy, and that it is being implemented consistently throughout the school
- ensuring adequate CPD is provided on issues concerning online safety within the school
- ensuring systems are in place to allow for monitoring and support of those in school who carry out monitoring roles
- ensuring 2x Senior Leaders are assigned as contacts to respond to Grade 4/5 safeguarding alerts generated through the Link2ICT Monitoring Service
- following procedures in the event of a serious online safety allegation made against or concerning a member of staff or pupils within the school.

4.3 Designated Safeguarding Lead (DSL)

4.3.1 Details of the school's Designated Safeguarding Lead (DSL) and deputy DSLs are set out in the school's Safeguarding and Child Protection Policy.

4.3.2 The DSL should be trained in Online 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 online contact with adults / strangers
- potential or actual incidents of grooming
- online bullying.

4.3.3 The DSL is responsible for:

- ensuring that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- ensuring that online safety incidents, including incidents of cyber-bullying - are logged and dealt with appropriately in line with this policy, the Behaviour Policy and Professional Learning Standards

- supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- working with the Headteacher, ICT Operations Manager and other staff, as necessary, to address any online safety issues, review incident logs and filtering/change control logs
- having and up to date awareness of online safety matters
- receiving and acting on Grade 4/5 safeguarding alerts generated through the Link2ICT Safeguarding Monitoring Service.

4.4 Pastoral Manager

4.4.1 The Pastoral Manager is responsible for:

- ensuring that online safety incidents, including incidents of cyber-bullying - are logged and dealt with appropriately in line with this policy, the Behaviour Policy and Professional Learning Standards
- monitoring and acting on monthly Grade 2 and weekly Grade 3 PCE Reports generated through the Link2ICT Safeguarding Monitoring Service.

4.5 ICT Operations Manager

4.5.1 The ICT Operations Manager is responsible for:

- putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep all pupils, staff and visitors safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- remaining at the forefront of online safety technical information and inform/update others as necessary
- supporting and advising the Designated Safeguarding Lead on technical online safety issues and systems
- reviewing and updating this policy annually, or sooner if necessary
- providing online safety induction and annual refresher training and guidance for staff
- ensuring data is held securely in line with the General Data Protection Regulation (GDPR)
- ensuring that monitoring software/systems are implemented and updated as required.
- ensuring that the school's technical infrastructure is secure and is not open to misuse or malicious attack, and that safety mechanisms are updated regularly
- ensuring that the school meets required online safety technical requirements and any Local Authority Online Safety Policy / Guidance that might apply – including the ServiceBirmingham Security Policy / Access Agreement
- ensuring that users may only access the networks and devices through a properly enforced password protection policy, in which passwords are regularly changed
- responding to requests to block access to potentially dangerous sites and, where possible, preventing downloading of potentially dangerous files.

4.6 All staff and volunteers

4.6.1 All staff, including contractors and agency staff, trainees and volunteers – are responsible for:

- ensuring they read, understand and implement this policy consistently and have signed the Staff Acceptable Use Policy/Agreement.
- agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use
- ensuring that online safety incidents, including incidents of cyber-bullying - are logged and dealt with appropriately in line with this policy, the Behaviour Policy and Professional Learning Standards
- ensuring all digital communication with pupils is on a professional level and carried out using only school systems
- ensuring they report any suspected misuse or problem for investigation / action / sanction
- ensuring that online safety issues are embedded in all aspects of the curriculum and other activities
- ensuring they supervise and monitor the use of all digital technologies in lessons and other school activities (where allowed)
- ensuring they moderate any digital communication tools they enable for pupil use; for example, when creating a class SharePoint site
- ensuring internet resources and searches are 'pre-screened' prior to use with pupils in lessons, and that processes are in place for dealing with any unsuitable material that is discovered
- ensuring that personal use of digital technologies, at any time, never brings personal professionalism or the school's reputation into disrepute
- appropriate safeguards are put in place to prevent pupils/others from unauthorised access to systems / personal information, including ensuring that privacy restrictions settings are appropriately set on personal social media accounts to reduce opportunity for access by pupils
- ensuring they use school resources appropriately, including printing/copying
- understanding that use of school devices/systems are monitored, and that enhanced monitoring may take place where unacceptable use is suspected.

4.7 Parents / Carers

4.7.1 All parents / carers are responsible for:

- playing a crucial role in ensuring their child understands the issues surrounding online safety
- ensuring their child has read, understood and agreed to the terms on acceptable use of the school's digital technologies and systems, and endorsing (by signature) the Pupil Acceptable Use Agreement
- monitoring their child's use of all digital technologies when not in school
- adhering to school restrictions on taking personal digital images whilst on school premises
- understanding that the school will automatically provide their child with access to digital technologies. Parents should contact the school if they have any concerns.

4.7.2 Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- UK Safer Internet Centre - https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues
- Childnet International - https://www.childnet.com/parents-and-carers/hot-topics

4.8 Pupils

4.8.1 Pupils are responsible for:

- ensuring they use digital technologies and the internet appropriately, following this online safety policy and the rules for acceptable use
- understanding the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online Safety Policy covers their actions out of school, if related to their membership of the school
- ensuring that all their digital communications with other pupils are appropriate, including when using personal devices/systems outside of school
- understanding how to report issues of abuse, misuse or access to inappropriate materials
- knowing and following school policy on the use of mobile devices, digital cameras and well as the use of images appropriately
- ensuring that personal use of digital technologies, at any time, is not detrimental to personal and school reputation
- ensuring that appropriate safeguards are put in place to prevent others from accessing personal information on digital technologies; for example – social media privacy restrictions settings
- ensuring they understand that school digital technologies and communications are monitored, and that enhanced monitoring may take place where unacceptable use is suspected
- ensuring they use school resources appropriately, including printing/copying.

4.9 Community Users, Contractors and Others

4.9.1 Community users, contractors, suppliers and others, who access school digital technologies / communications will be expected to sign an Acceptable Use Policy Agreement before being provided with access to school digital technologies.

5 Education and Training about Online Safety

5.1 Pupils

5.1.1 The purpose of using digital technologies in school is to raise educational standards, promote pupil achievement, support the professional work of staff and enhance school management functions.

5.1.2 Pupils are encouraged to use technology within school and outside of school to support their learning. It is important therefore to teach them the skills of using it appropriately, knowing and understanding the risks to allow them to take care of their own safety and security.

5.1.3 Pupils will be taught to:

- use digital technologies safely and respectfully
- recognise acceptable and unacceptable behaviour
- report concerns about content and contact
- protect their online identity and privacy
- understand how changes in technology affect safety

5.1.4 Online safety in the curriculum:

- Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum
- A planned online safety curriculum should be provided as part of Computing / PHSE / other lessons and should be regularly revisited
- Key online safety messages should be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities
- 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
- Pupils should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- 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.
- 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 practise that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.
- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites pupils visit.
- It is accepted that from time to time, for good educational reasons, pupils may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the ICT Support Staff 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. Removal of any restrictions required for these educational purposes need to be made at least 48 hours in advance so that any possible risks can be taken in to account and then cleared with DSL/SLT.

5.2 Parents / Carers

5.2.1 Parents / carers will receive information regarding online safety through school newsletters or other communications home. In addition, online safety information, and this policy will be available on our website.

5.2.2 If parents /carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the year group Pastoral Manager.

5.3 Staff / Volunteers

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced
- All new staff will receive online safety training as part of their induction programme, ensuring that they fully understand the school Online Safety Policy and Acceptable Use Policies / Agreements
- The DSL (or other nominated person) will receive regular updates through attendance at external training events (eg. from LA / other information / training sessions) and by reviewing guidance documents released by relevant organisations

- The DSL (or other nominated person) will provide advice / guidance / training to individuals as required.

5.4 Governors

5.4.1 Governors should take part in online safety training / awareness sessions, with particular importance for those who are members of any sub committee / group involved in technology / online safety / health and safety / safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the National Governors Association / LA or other relevant organisations.
- Participation in school training / information sessions for staff or parents.

6 Cyber-bullying

6.1 Cyber-bullying takes place online, such as through social media sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

6.2 Please refer to the school Behaviour Policy / Professional Learning Standards for more information on the school's cyber-bullying prevention work and sanctions.

7 Use of digital and video images - Photographic, Video

7.1 When using digital images, staff should inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

7.2 Written permission from parents or carers will be obtained before photographs of pupils are published on external public-facing media (school website, newsletter, social media, local press).

7.3 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 is not covered by the Data Protection Act). To respect everyone's privacy, and in some cases protection, these images must not be published / made publicly available on social media sites, nor should parents / carers comment on any activities involving other pupils in the digital videos / images.

7.4 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 or pupils should not be used for such purposes.

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

7.6 All users must not take, use, share, publish or distribute images of others without their permission.

7.7 Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images, and in line with Photographic Consent Records.

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

7.9 Pupil's work remains the property of Hodge Hill Girls' School, so can be published without permission.

8 Copyrighted Audio and Video

8.1 Licensing

8.1.1 Staff will only use commercial copyrighted audio and video for educational purposes, where the school has purchased the requisite licenses authorising such use. The following information is provided as a guide. Staff should ask if unsure.

- The school annually purchases licenses that allow movies/documentaries/music from selected studios, to be used in school for educational and "non-event[1]" use, for titles that have been purchased by the school or individuals, on CD/DVD media/other physical media.
- School usage rights do not extend to online streaming services, unless explicitly stated in the Terms and Conditions of the streaming service.
- Use of licenses must be justified for educational purposes. Recreational/non-curriculum use of these licenses is strictly prohibited.

8.2 Film Classification

8.2.1 Legal enforcement of film age classification only applies to cinemas / other public broadcasts. Schools are authorised to show content that is age-classified above the viewing audience – but there must be justification for educational purposes. Staff must make a judgement on how appropriate content is against the developmental age of pupils and the desired education outcomes, seeking support where appropriate.

8.3 Streaming Services

8.3.1 The default position is that legitimate streaming services (eg. Netflix, Spotify, Google Play, Apple Store) are not authorised for use in school. For further clarification, please see the ICT Operations Manager.

8.3.2 The following legitimate streaming services are permitted for use in school: BBC iPlayer, YouTube (free version only).

9 General Data Protection Regulation (GDPR)

9.1 Please refer to the school's Data Protection Policy (available from the school website).

9.2 Staff must:

- ensure that they, at all times, take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse
- understand that Data Protection Impact Assessments must be completed, and permission sought from authorised staff - when considering the use or purchase of new cloud-based systems. Staff must NOT sign up to systems without following due process and receiving written authorisation from the ICT Operations Manager.
- only use personal data on authorised secure devices/systems, ensuring that they properly log-off at the end of any session in which they are using personal data.

[1] Licensing restrictions; "non-event" = eg. Rewards movie, eg. Praise assembly. Must not involve members of the public. Parents are classed as members of the public in this case.

9.3 Physical external storage (eg USB sticks) must not be used for transfer of personal or sensitive information. There may be times where an exception to this is required, then any external storage must be encrypted at source, advice on this can be gained from the ICT Operations Manager. Staff are expected otherwise to use authorised secure transfer methods when transferring personal data, which includes:

- Direct access to files stored on OneDrive for Business/SharePoint
- Using "Share" Links in OneDrive for Business/SharePoint to distribute files.

10 Technical – infrastructure / equipment, filtering and monitoring

10.1.1 Please read and understand the School Technical Security Policy (available as an appendix at the end of this policy), which includes important information that expands on the following:

10.1.2 Technical Security:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- Appropriate security measures are in place to protect servers, firewalls, routers, wireless systems, workstations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data.
- The school infrastructure and individual workstations are protected by up to date virus software and security updates.
- Personal data must not be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- IT Systems must be secured or logged out if left unattended. It is the responsibility of individual users to ensure they logout of (or lock) user accounts if leaving systems unattended.
- School-owned equipment must NOT be removed from the school site without written permission from the Headteacher (or deputised). All device loans are subject to terms and conditions set out in the Device Loan Agreement.
- Staff are required to bring their school-owned laptops to school every day for teaching purposes. This also provides the system time to apply updates and security/virus patches where necessary.
- All equipment authorised for taking out of school is encrypted. Devices without encryptions must NOT be taken off-site. For clarification, see ICT Support staff.
- All staff will adhere to the "Controlled Assessments Technical Procedure" (available from ICT Support in school) when managing Controlled Assessments that require a technical solution.

10.1.3 Password Security:

- All users will have clearly defined access rights to school technical systems and devices.
- All users will be provided with a username and secure password by ICT Support.
- Users are responsible for the security of their username and password and under normal circumstances will be required to change their password every 45 days.

10.1.4 Filtering and Monitoring:

- Internet access is filtered for all users. Illegal content is filtered by the school's 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 to deal with requests for filtering changes. Seek advice from the ICT Operations Manager for more details.

- Internet filtering / monitoring ensures that children are safe from terrorist and extremist material when accessing the internet in school or on school-owned devices.
- "Over-blocking" will not lead to unreasonable restrictions as to what children can be taught.
- Authorised 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.

11 Mobile Devices

11.1 All staff, parents and pupils should read and understand the Mobile Devices Policy (available as an Appendix at the end of this policy), which includes important information that expands on the following:

- Mobile technology devices may be school owned/provided or personally owned and might include: smartphone, tablet, 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.
- All users should understand that the primary purpose of the use of mobile/personal devices in a school context is educational.
- The school allows:

	School-owned Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes[2]	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	Yes
No network access				Yes	Yes	Yes

- Secure "Guest wifi" is available for visitors/contractor's devices to enable them to carry out online work required as part of their visit. Staff/pupil personal devices will NOT be provided guest wifi access; school-owned devices are issued where staff require wifi access.

12 Social Media - Protecting Professional Identity

12.1 Personal use of social media can have an impact on personal reputation and the professional reputation of the school and its staff. All staff, parents and pupils should read and understand the Social Media Policy (available as an Appendix at the end of this policy).

[2] Pupils bringing mobile/smartphones into school must have them turned off/silent and put away and not used in school.

13 Communications

13.1 General Communications

13.1.1 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				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 /Smartphones may be brought to the school	/				/[3]			
Use of mobile/smartphones in lessons / meetings / training				/				/
Use of mobile/smartphones in social time		/						/
Taking photos on personal mobile/smartphones or other personal devices				/				/
Use of school-owned computers, tablets, laptops	/						/	
Taking photos on school-owned devices		/					/	
Use of other mobile school-owned devices eg. tablets		/					/	
Use of personal email addresses in school, or on school network		/					/	
Use of personal email for school business / work				/				/
Use of school email for school business / work	/				/			
Use of school email for personal emails				/				/
Use of messaging apps				/				/
Use of social media			/[4]	/				/
Use of blogs	/						/	

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

- The official school email service (currently Office 365 Mail/Outlook) and the official school virtual learning environment (currently Office 365/SharePoint) may be regarded as safe and secure and are monitored. Staff and pupils should therefore use only these systems to communicate with others when in school, or on school systems.
- Users need to be aware that communications are monitored.
- 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.
- Any digital communication between staff and pupils or parents / carers must be professional in tone and content. These communications may only take place on official, monitored school systems.

[3] Pupils bringing mobile/smartphones into school must have them turned off/silent and put away and not used in school.

[4] Specific named staff are authorised to use social media in support of safeguarding investigations, and to monitor the school reputation online.

Personal email addresses, text messaging[5] or social media/whatsapp/messenger must not be used for these communications.

- All communication between staff and pupils must be via school communication systems until the pupil leaves Further Education (aged 18). Staff and ex-staff use of personal communication systems with (ex-)Hodge Hill Girls' School pupils under the age of 18 is strictly prohibited.
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff.
- School communication systems are provided primarily to support learning and other school business functions. Therefore, it is important that such systems are not used in an abusive manner.
- Users must not communicate personal or other information about themselves or others that could cause harm/embarrassment to anyone or the school's reputation.
- Users should not assume that a communication is private and confidential, even if marked as such. School communication systems are monitored and filtered for appropriate use. The confidentiality of communication may be compromised at any point along the way unless the communications are encrypted.
- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account. This also applies if staff employment ceases.
- Pupils are not permitted to follow or engage with current or prior staff of the school on any personal social media network account.

13.2 Email

13.2.1 Staff and pupils will be provided with individual school email addresses for educational use:

- Use of personal communication systems (e.g. Hotmail, Yahoo Mail, Facebook) between school users, or for school business is prohibited.
- The forwarding of chain/spam communications (eg. chain letters, jokes) is not permitted.
- Sensitive information or data must not be sent in school communications without encryption. It is the user's responsibility to ensure that data is protected to school standards before sending. If unsure, seek advice from ICT Support.
- "Sharing" files from OneDrive/SharePoint is a secure and appropriate way to send files containing sensitive information. The traditional "Attachment" of files to email is NOT a secure or appropriate way to send files containing sensitive information.
- The school enforces email storage quotas on all user email accounts. It is the user's responsibility to ensure communications/files are archived/printed or deleted to ensure accounts stay within the allocated limit. This should be done on a daily basis, as communications are accessed rather than waiting for limits to be reached. In the event that a user's quota limit is reached/exceeded the user is not able to send/receive communications until the user takes action to reduce their quota usage. Training is available to help users to manage their quotas.
- Users are responsible for any repercussions that relate to not being able to receive important communications, if they do not manage their quota appropriately.
- Staff must not set “auto-forward”/”redirect” options to redirect school email to another personal email account. School monitoring systems will flag this up to ICT Support for investigation.

[5] The school uses an SMS Messaging service (currently SchoolComms) to communicate one-way with Parents via text messaging. This is the only authorised text-messaging service.

13.3 Phishing

13.3.1 The following guidance is provided to assist school email users on how to identify if they have received a phishing email, and the action they should take:

- The school employs virus-protection and monitoring systems that prevent 99% of spam and phishing email from reaching recipients. 100% automated protection is not possible, so all school email users have a duty to be able to identify if they may have received a phishing email, and the actions they should take.
- "Phishing" is a criminal activity using various techniques to manipulate users into performing actions or divulging confidential information that users would not normally provide. Phishing emails may appear to be from a trustworthy source, but are designed to trick the email recipient into disclosing sensitive, private and confidential information. By clicking on an active link in a phishing email, the recipient may be directed to a fraudulent web site that attempts to acquire personal or private information, or possibly infect their computer with malicious software.

13.3.2 Signs that an email may be a phishing attempt:

- The email contains obvious spelling errors. Phishers do this intentionally to avoid spam filters.
- Links to the website contain all or part of a real entity's name, or web address, but the link itself is not identical to that of the legitimate website.
- The email address that the email comes from, contain all or part of a real entity's name, or email domain, but the address itself is not identical to that of the legitimate email domain/address.

13.3.3 Checks that school email users should make on suspected phishing emails:

- Hover over, but don't click, on the link in the email. Whilst hovering, review the address information in the status bar located at the bottom of the browser window/page. It may not point to a legitimate website.
- Links in emails are only there for user convenience. Users can go direct to a legitimate website by typing a legitimate website address in their browser, rather than clicking on a suspect link.
- Identifying the source address of an email is harder to achieve. It's very easy for phishers to state that they are from a legitimate company's email address, when they are not. The most effective way to check the source of an email is to select the option to "View Source" or "View Original" and inspect the email headers. ICT Support can assist with this.

14 Dealing with Incidents

14.1.1 Some internet activity eg. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. Other activities eg. cyberbullying 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 context, either because of the age of the users or the nature of those activities.

14.2 Unsuitable / inappropriate activities

14.2.1 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 certain usage as follows:

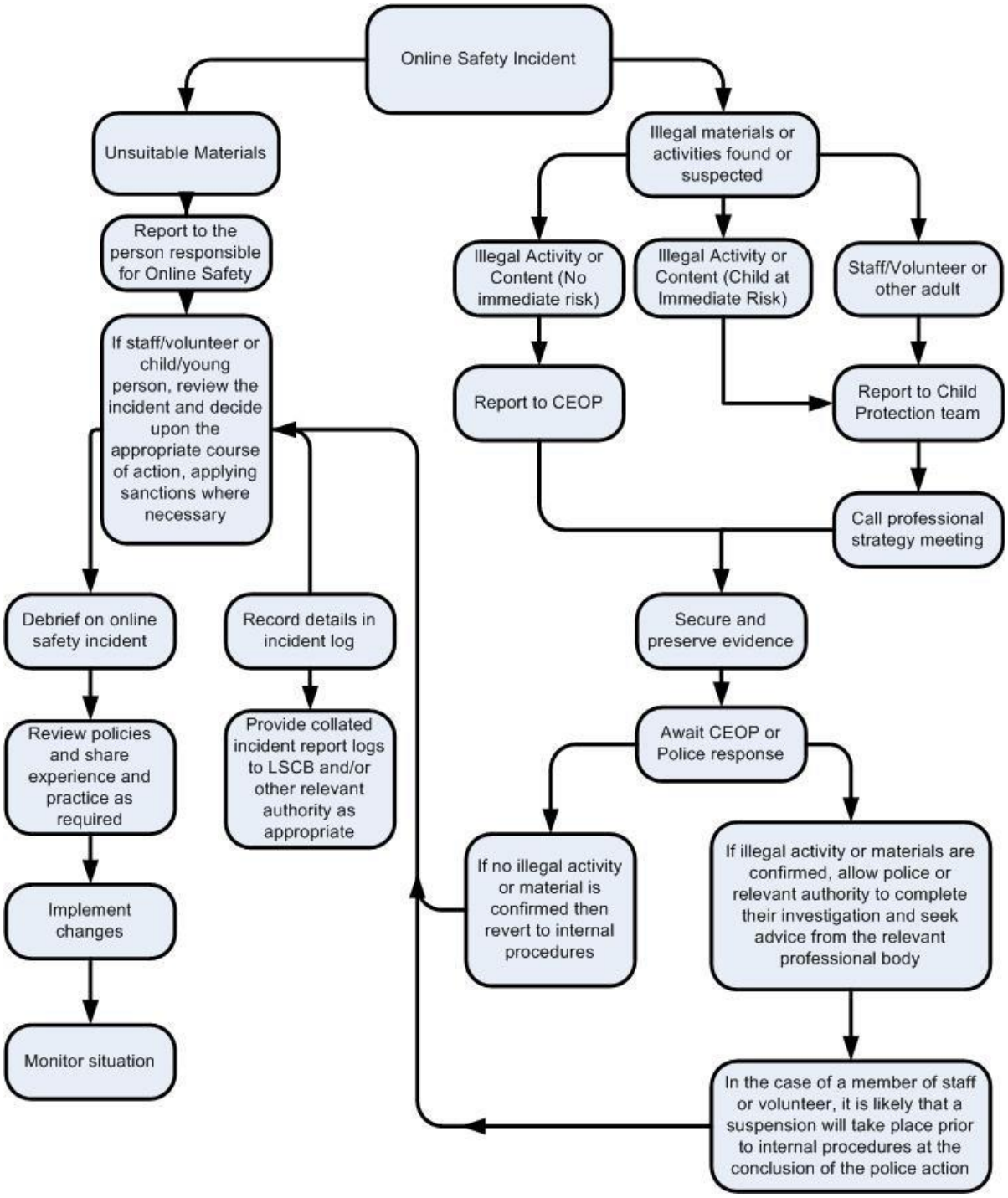
User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and Illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images – The making, production or distribution of indecent images of children. Contrary to the Protection of Children Act 1978					/
	Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.					/
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character). Contrary to the Criminal Justice and Immigration Act 2008.					
	Promotion of extremism or terrorism					/
	Pornography				/	
	Promotion of any kind of discrimination				/	
	Threatening behaviour, including promotion of physical violence or mental harm				/	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				/	
Using school systems to run a private business					/	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school					/	
Infringing copyright					/	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)					/	
Creating or propagating computer viruses or other harmful files					/	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet / network)					/	
Use of school equipment/devices without permission					/	
On-line gaming (educational)			/			
On-line gaming (non educational)					/	
On-line gambling					/	
On-line shopping / commerce – for school business (for the purposes of comparing quotes to achieve value for money in school)				/		
On-line shopping / commerce – personal use					/	
Legal File sharing related to learning and other school business				/		
Use of social media					/	
Use of messaging apps					/	
Use of video broadcasting eg YouTube			/			

14.3 Responding to Incidents of Misuse

14.3.1 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).

14.4 Illegal Incidents

14.4.1 If there is any suspicion that the website(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) for responding to online safety incidents and report immediately to the police.



14.5 Other Incidents

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

- Have more than one senior member of staff / volunteer involved in the process.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded.
- 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 child sexual abuse - see below).
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
  - Internal response or disciplinary procedures.
  - Involvement by Local Authority or national / local organisation (as relevant)
  - Police involvement and/or action.

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

- Incidents of 'grooming' behaviour
- The sending of obscene materials to a child
- Adult material which potentially breaches the Obscene Publications Act
- Criminally racist material
- Promotion of terrorism or extremism
- Other criminal conduct, activity or materials.

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

14.5.3 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 forms should be retained by the group for evidence and reference purposes.

14.6 Process for Dealing with Offensive Material About Staff

14.6.1 If staff discover that, arising from employment as an education professional, a website contains incorrect, inappropriate or inflammatory written material relating to them, or images of which have been taken and/or which are being used without permission, then staff should immediately report this to the Headteacher:

- The Headteacher will conduct an investigation.

- If it is evidenced, in the course of the investigation, that an identified pupil(s) submitted material to the website, then the pupil(s) will be disciplined in line with the Behaviour Policy / Professional Learning Standards, and the pupil/parent will be asked to amend or remove the offending content.
- Where appropriate, the investigating officer should approach the website hosts to request that the material is either amended or removed. If the website requires the individual who is complaining to do so personally, the school should give their full support and assistance.
- Checks should be carried out to verify if the requested amendments or removals were made. If the websites will not cooperate, the investigating officer should contact the "UK Safer Internet Centre's Professionals Online Safety Helpline" (0844 381 4772) to seek further support and guidance on future course of action. The UK Safer Internet Centre has contacts with law enforcement agencies and technology companies that can be useful in achieving a satisfactory outcome.
- If the material is threatening and/or intimidating, the Headteacher should consider reporting the matter to the police (with the member of staff's consent).

14.7 School Actions & Sanctions

14.7.1.1 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:

Pupil Incidents	Refer to class teacher / tutor	Refer to Pastoral Team / DSL	Refer to Headteacher	Refer to Police	Refer to Technical Support Staff for action (filtering / security)	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).		/	/	/			/		/
Loss / theft / damage to school equipment		/	/	/	/	/		/	/
Use of school equipment/devices without permission	/	/						/	
Unauthorised use of non-educational sites during lessons	/				/			/	
Unauthorised / inappropriate use of mobile phone / digital camera / other mobile device	/	/						/	/
Unauthorised use of social media / messaging apps / personal email	/	/						/	
Unauthorised downloading or uploading of files	/	/			/			/	
Allowing others to access school network by sharing username and passwords	/	/			/		/	/	
Attempting to access or accessing the school network, using another pupil's account	/	/			/	/	/	/	

Pupil Incidents	Refer to class teacher / tutor	Refer to Pastoral Team / DSL	Refer to Headteacher	Refer to Police	Refer to Technical Support Staff for action (filtering / security)	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction eg detention / exclusion
Attempting to access or accessing the school network, using the account of a member of staff			/		/	/	/	/	/
Corrupting or destroying the data of other users		/			/			/	
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature	/	/			/			/	/
Continued infringements of the above, following previous warnings or sanctions			/			/		/	/
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		/						/	
Using proxy sites or other means to subvert the school's filtering system		/			/			/	
Accidentally accessing offensive or pornographic material and failing to report the incident	/	/						/	
Deliberately accessing or trying to access offensive or pornographic material		/						/	/
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		/						/	

Staff Incidents	Refer to line manager	Refer to Headteacher	Refer to LA / HR	Refer to Police	Refer to Technical Support Staff for action (filtering / security)	Warning	Suspension	Disciplinary Action
Deliberate actions to breach data protection or network security rules		/	/			/	/	/
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		/					/	/
Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		/				/	/	/
Using personal email / social media / instant messaging / text messaging to carry out digital communications with pupils		/				/	/	/
Actions which could compromise the staff member's professional standing		/				/	/	/
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		/	/			/	/	/
Using proxy sites or other means to subvert the school's filtering system		/					/	/
Accidentally accessing offensive or pornographic material and failing to report the incident		/				/		
Deliberately accessing or trying to access offensive or pornographic material		/	/				/	/
Breaching copyright or licensing regulations		/				/		
Continued infringements of the above, following previous warnings or sanctions		/	/				/	/

14.8 Other Guidance

- Third party complaints, or from parents concerning activity that occurs outside the normal school day, should be shared with the Headteacher.
- Minor pupil offences such as being off-task visiting games or email websites will be handled by the teacher in situ by invoking the school Behaviour Policy / Professional Learning Standards.
- Serious breaches of this policy by pupils will be treated as any other serious breach of conduct in line with the Behaviour Policy / Professional Learning Standards. Referral to Pastoral Managers / Leadership Team may be appropriate at this level.
- Pupil policy breaches relating to bullying, drugs misuse, abuse, suicide and serious health problems must be reported to the nominated Child Protection Officer and action taken in line with anti-bullying and child protection policies. There may be occasions when the police and/or local authority agencies need to be involved.
- Breaches of this policy by staff will be investigated by the Headteacher. Action will be taken under Birmingham City Council's Disciplinary Policy where a breach of professional conduct is identified. Incidents will be fully investigated, and appropriate records made on staff files with the ultimate sanction of summary dismissal reserved for the most serious of cases involving gross misconduct. All monitoring and investigation of staff use will be carried out by 2x senior members of staff.

- For pupils, the removal of internet access will not be a sanction that is applied unless it is justified as a last resort. Where possible, limited access can be enforced for a set period commensurate with the breach of conduct.
- Parents are asked to work in partnership with staff to resolve issues and will be informed of the school's complaints procedure.
- Advice on handling Online Safety incidents can be sought via the nominated Online Safety representative in School, and via the Online Safety team at the LA (telephone 0121 303 5100).

15 Development / Monitoring / Review

15.1 This Online Safety Policy has been developed in consultation with:

- School Leadership Team
- Staff - including Teachers, Support Staff, Technical staff
- Governors
- Parents, Carers and Pupils

15.2 The school will monitor the impact of the policy once per term using:

- Logs of reported incidents
- Monitored logs of activity (including sites visited and screen captures) / filtering
- Surveys / questionnaires of pupils, parents/carers, staff.
- The Governing Body will receive a report on the implementation of the Online Safety Policy once per term.

15.3 The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place.

16 Links with Other Policies

16.1 This Online Safety Policy is linked to the following policies:

- School Technology Security Policy (appended to this policy)
- Electronic Devices – Searching and Deletion Policy (appended to this policy)
- Mobile Technologies Policy (appended to this policy)
- Social Media Policy (appended to this policy)
- Anti-bullying Policy (available from school website)
- Access Control Policy (available to staff in school from internal policies site)
- Behaviour Policy / Professional Learning Standards (available from school website)
- Data Protection Policy (available from school website)
- Information Security Policy (available to staff in school from internal policies site)
- Safeguarding and Child Protection Policy (available from school website)

Hodge Hill Girls' School

Online Safety Policy

Appendices / Supporting Documentation

Sections A1 - A5 removed and moved to Student AUP

A6 Online Safety Policy – Summary of Key Points for Staff

A6.1.1 **Policy/Scope** – All staff are required to annually read, understand and sign the Staff Acceptable Use Policy Agreement. All staff are required to read, understand and comply with the Online Safety Policy, which applies to use of school digital technologies in and out of school, as well as personal use of any digital technologies/social media at any time, where such personal use could bring personal/professional/school reputation into disrepute. Refer to "3. Scope of the Policy" in the Online Safety Policy.

A6.1.2 **Photos/Video** – do not use personal devices for taking images of pupils. Use school-owned devices. Always check photo permissions list. Photos must not be published publicly (eg. School Website) without written approval. Refer to "7. Use of digital and video images" in the Online Safety Policy.

A6.1.3 **Streaming Services** – The default position is that legitimate streaming services (eg. Netflix) are NOT authorised for use in school. Exceptions apply. Refer to "8. Copyrighted Audio and Video" in the Online Safety Policy.

A6.1.4 **GDPR** – Staff are NOT authorised to sign the school up to new Cloud-based services; staff should submit a "Data Protection Impact Assessment" and seek permission from the ICT Operations Manager. Staff must not transfer files containing sensitive/personal information via regular email attachment or external physical storage devices (eg. USB storage) due to the risk of Data Protection breach; instead staff should "share" files securely using Office 365, or another form of authorised encryption. Refer to "9. GDPR" in the Online Safety Policy.

A6.1.5 **Technical / Password Security** – Computers must not be left logged in unattended; staff should "lock" computers or logout. Staff must set complex passwords using a mixture of uppercase, lowercase, numbers and non-alphanumeric characters. School-owned equipment must NOT be removed from the school site without permission. Staff are required to connect staff laptops to the school network at least once every 2-weeks. Staff must NOT attempt to connect personal devices to the school network (physical or wifi). Refer to "10.1.2 Technical Security", "10.1.3 Password Security" and "11. Mobile Devices" in the Online Safety Policy.

A6.1.6 **Safeguarding Filtering and Monitoring** – All staff/pupil use of school-owned computers is monitored via "PCE" monitoring software and the Link2ICT Safeguarding Monitoring Service. The Pastoral/DSL Team are alerted to pupil PCE Captures. The Head teacher is alerted to staff PCE captures. Staff are required to use AB Tutor in IT rooms to control and monitor pupil IT usage. All internet access in school is filtered at Local Authority and School level. Refer to "10.1.4 Filtering and Monitoring" in the Online Safety Policy.

A6.1.7 **Communications/Social Media** – All communication between staff and pupils must be via official sanctioned school systems (Office 365) until the pupil leaves Further Education (aged 18). Staff and ex-staff use of personal email/social media with pupils and ex-pupils is strictly prohibited. If staff receive unwarranted communication from (suspected) parents/pupils to personal email/social media, staff must NOT respond, but instead seek advice immediately. Refer to "13. Communications" in the Online Safety Policy.

A6.1.8 **Phishing** – Schools/staff are currently at a particularly high risk of being targeted for "Phishing attacks", which is criminal activity aimed at manipulating users to perform actions or divulge information that users would not normally provide – commonly received via email. Staff need to understand and be alert to the signs of a phishing attack, and ensure no action is taken that could jeopardise the security of their accounts or the technical security of the school. Phishing attacks should be reported to ICT Support. Refer to "13. Phishing" in the Online Safety Policy.

A7 Staff (and Visitor) Acceptable Use Policy Agreement

A7.1 School Policy

A7.1.1 This Acceptable Use Policy Agreement is intended to ensure:

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

A7.1.2 The school will try to ensure that staff and visitors will have good access to digital technology to enhance their work, to enhance learning opportunities for pupils and will, in return, expect staff and visitors to agree to be responsible users.

A7.1.3 All digital technology use in and out of school is bound by the Online Safety Policy.

A7.1.4 All staff and visitors are advised to read the following related documents and policies:

- Online Safety Policy
- School Technical Security Policy
- Access Control Policy / Acceptable Use Agreement
- Information Security Policy
- Behaviour Policy / Professional Learning Standards
- Data Protection Policy
- Staff Professionalism Document

A7.2 Acceptable Use Policy Agreement

A7.2.1 I accept and will abide by the rules set out in this agreement and the Online Safety Policy. I also accept and will abide by Hodge Hill Girls' School's Access Control Acceptable Use Agreement.

A7.2.2 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 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 online safety in my work with young people.

A7.2.3 For my professional and personal safety:

- I understand that the school will monitor my use of the systems, devices and digital communications.
- I understand that the rules set out in this agreement also apply to my use of these technologies out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will not use the systems for personal or recreational use.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

A7.2.4 I will be professional in my communications and actions when using school 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. Where these images are published (eg on the school website / learning platform) it will not be possible to identify by name, or other personal information, those who are featured.
- I will not use social media sites in school or on school-owned equipment, unless I have been given explicit permission.
- I will only communicate with staff, visitors, pupils and parents / carers using official school systems. Any such communication will be professional in tone and manner. (See Staff Professionalism Document).
- I will not engage in any online activity that may compromise my professional responsibilities.

A7.2.5 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 personal mobile devices (eg. smartphone / 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 operating system updates and anti-virus software, and are free from viruses.
- If I am issued with a school-owned device (eg. staff laptop, tablet), I will connect it to the school network at least once per fortnight, to enable monitoring of use outside school.
- I will not attempt to connect personal devices to the school network (wired or wireless) due to the security risk of cross-contamination of malware/viruses – unless I have explicit, written permission from the school
- 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.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy and Privacy Notices. Where personal data is transferred outside the secure school 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 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.

A7.2.6 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).

A7.2.7 I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy Agreement 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 and / or the Local Authority and in the event of illegal activities the involvement of the police.

A7.2.8 Please complete the sections on the next page to show that you have read, understood and agree to the rules included in this Acceptable Use Policy Agreement.

A7.3 Staff / Visitor Acceptable Use Policy Agreement Form

A7.3.1 This form relates to the Staff / Visitor Acceptable Use Policy (AUP) Agreement, to which it is attached.

A7.3.2 Please complete the sections below to show that you have read, understood and agree to the rules included in the Staff / Visitor Acceptable Use Policy Agreement. If you do not sign and return this agreement, access will not be granted to school systems.

A7.3.3 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.

A7.3.4 I agree to follow the guidelines set out in Staff / Visitor Acceptable Use Policy and the Online Safety Policy.

Staff / Visitor Name:	
Signed:	
Date:	

A8 Record of Reviewing Devices / Internet Sites

Group:	
Date:	
Reason for Investigation:	

Details of 1st reviewing person		**Details of 2nd reviewing person**	
Name:		**Name:**	
Position:		**Position:**	
Signature:		**Signature:**	

Name and location of computer used for review (for web sites):	

Web site(s) address / device	**Reason for concern**

Conclusion	**Action proposed or taken**

A9 Reporting Log

Group:

Date	Time	Incident	Action Taken?		Incident Reported By	Signature
			What?	By Whom?		

A10 School Technical Security Policy

A10.1 Introduction

A10.1.1 Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The school will be responsible for ensuring that the school infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the school's policies)
- access to personal data is securely controlled in line with the school's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of school systems
- there is oversight from senior leaders and these have impact in policy and practice.

A10.2 Responsibilities

A10.2.1 The management of technical security will be the responsibility of the ICT Operations Manager.

A10.2.2 All staff are responsible for the security of data, usernames and passwords that they generate or have access to.

A10.3 Technical Security

A10.3.1 The school will be responsible for ensuring that the school infrastructure / network is as safe and secure as reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people receive guidance and training and will be effective in carrying out their responsibilities:

- School technical systems will be managed in ways that ensure that the school meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of school technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc. from malicious attempts which might threaten the security of the school systems and data – including system updates and robust anti-virus protection.
- Responsibilities for the management of technical security are assigned to the ICT Operations Manager.
- The ICT Operations Manager is 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.
- Mobile device security and management procedures are in place for school-owned devices.
- School technical staff ensure that monitoring software records the activity of users on the school technical systems and users are made aware of this in the Acceptable Use Agreement.
- Remote management tools are used by staff to control workstations and view users activity.
- An appropriate system is in place for users to report any actual / potential technical incident to the ICT Operations Manager.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto the school system.

- An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on school devices that may be used out of school.
- An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on school devices.
- The school infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.
- Personal data cannot be sent over the internet or taken off the school site unless safely encrypted or otherwise secured.
- Hodge Hill Girls' School reserves the right to confiscate devices that it suspects contain viruses, or that pose a risk to system security. ICT Support staff will request permission from the device owner to have the device scanned and cleaned. Where the device owner permits this, the cleaning operation will be carried out at risk to the device owner. If the device owner does not give permission, the device will be confiscated and parents contacted to collect the device – to protect the integrity of the school network.

A10.4 Password Security

A10.4.1 A safe and secure username / password system is essential if "Technical Security" is to be established and will apply to all school technical systems, including network, email and Virtual Learning Environment (VLE).

- The management of the password security policy will be the responsibility of the ICT Operations Manager.
- All users will have clearly defined access rights to school technical systems and devices. Details of the access rights available to groups of users will be recorded by the ICT Operations Manager.
- All school networks and systems will be protected by secure passwords that are regularly changed.
- The "master / administrator" passwords for the school systems, used by ICT Support staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg. school safe. Consideration should also be given to using two factor authentication for such accounts.
- All users (adults and young people) will have responsibility for the security of their usernames and passwords, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords for new users, and replacement passwords for existing users will be allocated by ICT Support Staff. Username and Passwords to the MIS are managed by the Data Manager. Any changes carried out must be notified to the manager of the Password Security Policy (above).
- Requests for password changes should be authenticated by the ICT Operations Manager to ensure that the new password can only be passed to the genuine user.
- All users will be provided with a username and password by the ICT Operations Manager who will keep an up to date record of users and their usernames.
- The password should be a minimum of 8 characters long and must include three of – uppercase character, lowercase character, number, special characters.
- Users will be required to change their password every 45 days.
- Pupils will be taught the importance of password security.
- Passwords must not include proper names or any other personal information about the user that might be known by others.
- The account should be "locked out" following five successive incorrect log-on attempts.
- Temporary passwords eg. used with new user accounts, or when users have forgotten their passwords, shall be enforced to change immediately upon the next account log-on.
- Passwords shall not be displayed on screen, and shall be securely hashed (use of one-way encryption).

- Passwords should be different for different accounts.
- All passwords should be changed at least every 45 days.
- Should not be reused for 6 months and be significantly different from previous passwords created by the same user. The last five passwords cannot be reused.

A10.5 Filtering

A10.5.1 The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use. It is important that the school has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this school.

- The responsibility for the management of the school's filtering policy will be held by the ICT Operations Manager. They will manage the school filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.
- All users have a responsibility to report in writing immediately to ICT Support any infringements of the school's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.
- Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- The school maintains and supports 3x 'levels' of filtering that help it meet its' statutory requirements to ensure the safety of pupils and staff:
    - Local Authority Level – managed filtering service provided by the Internet Service Provider (ISP - currently "Link2ICT/Exa"). Filtering decisions at this level affect all schools that use this ISP.
    - School Level - joint-managed filtering service provided by the ISP using "Surfprotect". Filtering decisions at this level affect all users in this school.
    - User Level – joint-managed filtering service provided by the ISP using "Surfprotect". Filtering decisions at this level affect individual users, or groups of users.
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Headteacher (or other nominated senior leader).
- Internet access is filtered for all users and devices that connect through the school network. Differentiated internet access is available for staff and customised filtering changes are managed by the school.
- Mobile devices that access the school internet connection (whether school or personal devices) will be subject to the same filtering standards as other devices on the school systems.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by ICT Support staff in consultation with the DSL, who is a member of the Leadership Team. Such requests can only be agreed by a member of the Leadership Team. If the request is agreed, this action will be recorded and logs of such actions shall be reviewed regularly.
- Illegal content is filtered by the Internet Service Provider employing the Internet Watch Foundation CAIC list and other illegal content lists. Filter content lists are regularly updated and internet use is logged and frequently monitored.

A10.5.2 Changes to the Filtering System

- Requests for filtering/unfiltering of a specific site will only be considered on the basis of safeguarding risk and educational merit of access.
- Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to ICT Support, by emailing helpdesk@hodgehgs.bham.sch.uk. This will log a helpdesk ticket for ICT Support's attention. If the request is urgent for safeguarding reasons, speak to ICT Support staff directly.
- Urgent requests can normally be processed and acted on within 2 hours. Non-urgent requests will take up to 5-days to process and take action.
- ICT Support staff should ensure that the request is recorded appropriately. Refer to "Record of Reviewing Devices / Internet Sites" for details of information that should be recorded.
- ICT Support should consult with, and ensure any changes to filtering are authorised by, the DSL (or nominated member of Leadership Team).
- When a course of action is determined by the DSL, ICT Support should give consideration as to the 'level' to which filtering changes should be applied:
  - Local Authority Level – ICT Support can refer the filtering change request to the Internet Service Provider for implementing on behalf of all local schools.
  - School Level – ICT Support can implement the filtering change request using the SurfProtect Administration to affect all school users.
  - User Level – ICT Support can implement the filtering change request using SurfProtect Administration to affect an individual user or group of users. These changes will take longer than School Level changes.
- ICT Support should provide feedback on the outcome/action taken to the requesting user via the original helpdesk ticket – whether the request has been approved or denied.

A10.6 Monitoring

A10.6.1 No filtering system can guarantee 100% protection against access to unsuitable sites. The school will therefore monitor the activities of users on the school network and on school equipment as indicated in the School Online Safety Policy and the Acceptable Use Agreement. Monitoring will take place as follows:

- At the Local Authority level, the Internet Service Provider records logs of websites visited by computer address and date/time. The ISP employs the Internet Watch Foundation CAIC list to ensure that certain categories of websites and content are blocked to prevent access to illegal and inappropriate content categories such as "pornography", "self-harm", "illegal", "drugs", "social-networking" and "age-restricted". Website category lists are updated on a daily basis.
- At the school level, "Smoothwall", formely known as PCE, is installed on all computers to monitor usage. PCE captures screen shots that include words or phrases on-screen that match high-risk libraries/categories, or captures user attempts to access blocked websites.
- The school subscribes to the "Safeguarding Monitoring Service" provided by the Local Authority (ServiceBirmingham). On a daily basis, ServiceBirmingham staff monitor and review the PCE-generated screen captures of computer usage by all school users.
- The pupil screen captures are then 'graded', capture-records updated, and action taken as indicated below:

Grade	Descriptor	Managed Service Response	School Response[6]
Grade 1	False positive - no problem	Captures graded. Records updated.	No action.

[6] School response – in the case of pupils, the Pastoral Manager or DSL responds. In the case of staff, the Headteacher responds.

Grade	Descriptor	Managed Service Response	School Response[6]
Grade 2	Inappropriate content or behaviour, but not safeguarding-related	Summary emailed to School Pastoral Managers – monthly	Pastoral Managers: Summary emails reviewed monthly and action taken where appropriate.
Grade 3	Potentially unsafe content or behaviour	Summary emailed to School Pastoral Managers – monthly	Pastoral Managers: Summary emails reviewed weekly and action taken where appropriate.
Grade 4	Serious, non-urgent child safeguarding threat	Incident summary emailed to DSL and Headteacher for action – as soon as possible after incident discovered.	DSL: Investigates incident / takes action during working hours, as soon as alerted.
Grade 5	Serious and urgent child safeguarding threat – present or imminent danger	Direct phone call with Headteacher or DSL – immediately as incident discovered.	DSL: Investigates incident / takes action immediately, as soon as alerted.

Table: PCE Captures – Grading and Response

- PCE is a managed ICT System that closely integrates with several other ICT systems. ICT Support staff have access to PCE in order to ensure the smooth-running of the system, and to enforce new filtering restrictions as and when required. All school laptops have PCE installed to enable the school to meet its obligation to monitor use of school equipment taken off-site. PCE operators have received training externally or as part of INSET.
- At the teaching group level, "NetSupport School" is installed in all ICT suites. NetSupport School is an effective classroom management tool that enables staff to control access to applications/websites in-class, and makes monitoring activity easier. NetSupport School can also be used to distribute documents to pupils in a single- click. NetSupport School allows staff to manage pupil computers by remotely viewing pupils' screens and taking control of mouse/keyboard movements if required. The use of NetSupport School on staff computers is not permitted. Staff computers are monitored effectively through PCE and NetSupport DNA. The ICT Operations Manager has responsibility for managing and monitoring NetSupport School & NetSupport DNA. Staff receive induction training on how to use NetSupport School, and additional support is available and targeted where required.

A10.7 Further Guidance

- Schools in England (and Wales) are required "to ensure children are safe from terrorist and extremist material when accessing the internet in school, including by establishing appropriate levels of filtering" (Revised Prevent Duty Guidance: for England and Wales, 2015).
- Furthermore the Department for Education published proposed changes to "Keeping Children Safe in Education' for consultation in December 2015. Amongst the proposed changes, schools will be obligated to "ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the school or colleges IT system" however, schools will need to "be careful that "over blocking" does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding."
- In response UKSIC produced guidance and information on "Appropriate Filtering".

A10.8 Training / Awareness

A10.8.1 Members of staff will be made aware of the school's Technical Security Policy at induction, through the school's online safety policy, through the Acceptable Use Agreement, and through staff meetings, briefings, INSET.

A10.8.2 Pupils will be made aware of the school's Technical Security Policy in lessons, and through the Acceptable Use Agreement.

A10.8.3 Parents will be made aware of the school's Technical Security Policy through the Acceptable Use Agreement and through parent meetings/briefings/newsletter.

A10.9 Audit / Reporting

A10.9.1 The ICT Operations Manager will ensure that full records are kept of:

- User IDs and user log-ins
- Security incidents related to this policy
- Web-access logs

A10.9.2 The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision.

A11 Electronic Devices – Searching and Deletion Policy

A11.1 Introduction

A11.1.1 The changing face of digital technologies and ever increasing pupil use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to schools by statute to search pupils in order to maintain discipline and ensure safety.

- The particular changes we deal with here are the added power to search for items 'banned under the school rules' and the power to 'delete data' stored on seized electronic devices.
- Items banned under the school rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).
- An item banned by the school rules may only be searched for under these new powers if it has been identified in the school rules as an item that can be searched for.
- The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a 'good reason' to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the school rules.
- Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.
- The Headteacher must publicise the Behaviour Policy / Professional Learning Standards, in writing, to staff, parents / carers and pupils at least once a year.

A11.2 Relevant legislation:

- Education Act 1996
- Education and Inspections Act 2006
- Education Act 2011 Part 2 (Discipline)
- The School Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
- Health and Safety at Work etc. Act 1974
- Obscene Publications Act 1959
- Children Act 1989
- Human Rights Act 1998
- Computer Misuse Act 1990

- This list is not intended to be exhaustive.

A11.3 Responsibilities

A11.3.1 The Headteacher is responsible for ensuring that the school policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

A11.3.2 The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices:

- Designated Safeguarding Lead (DSL)-trained staff

A11.3.3 The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

A11.4 Training / Awareness

- Members of staff should be made aware of the school's policy on "Electronic devices - searching and deletion" at induction and at regular updating sessions on the school's online safety policy
- Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.
- Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

A11.5 Search

A11.5.1 The school Behaviour Policy / Professional Learning Standards refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

- Pupils are allowed to bring personal mobile devices to school on condition that they are handed in on arrival and collected at the end of the school day. Pupil personal devices must not be used on the school site..
- If pupils breach these rules, the sanctions for breaking these rules can be found in the Behaviour Policy / Professional Learning Standards.
- Authorised staff (defined in the responsibilities section above) have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules:
    - Searching with consent - Authorised staff may search with the pupil's consent for any item
    - Searching without consent - Authorised staff may only search without the pupil's consent for anything which is either 'prohibited' (as defined in Section 550AA of the Education Act 1996) or appears in the school rules as an item which is banned and may be searched for.

- In carrying out the search:
    - The authorised member of staff must have reasonable grounds for suspecting that a pupil is in possession of a prohibited item i.e. an item banned by the school rules and which can be searched for.
    - The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search.
    - The authorised member of staff should take care that, where possible, searches should not take place in public places e.g. an occupied classroom, which might be considered as exploiting the pupil being searched.
    - The authorised member of staff carrying out the search must be the same gender as the pupil being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the pupil being searched.
    - There is a limited exception to this rule: Authorised staff can carry out a search of a pupil of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

- Extent of the search:
  - The person conducting the search may not require the pupil to remove any clothing other than outer clothing.
  - Outer clothing means clothing that is not worn next to the skin or immediately over a garment that is being worn as underwear (outer clothing includes hats; shoes; boots; coat; blazer; jacket; gloves and scarves).
  - 'Possessions' means any goods over which the pupil has or appears to have control - this includes desks, lockers and bags.
  - A pupil's possessions can only be searched in the presence of the pupil and another member of staff, except where there is a risk that serious harm will be caused to a person if the search is not conducted immediately and where it is not reasonably practicable to summon another member of staff.
  - The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.
  - Use of Force - force cannot be used to search without consent for items banned under the school rules regardless of whether the rules say an item can be searched for.

A11.6 Electronic devices

A11.6.1 An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so.

- The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.
- If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:
  - child sexual abuse images (including images of one child held by another child)
  - adult material which potentially breaches the Obscene Publications Act
  - criminally racist material
  - other criminal conduct, activity or materials

A11.7 Deletion of Data

A11.7.1 Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

- If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of school discipline) or whether the material is of such seriousness that it requires the involvement of the police.
- A record should be kept of the reasons for the deletion of data / files.

A11.8 Care of Confiscated Devices

A11.8.1 School staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices.

A11.9 Audit / Monitoring / Reporting / Review

- The Deputy Headteacher / Designated Safeguarding Lead will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files. (a template log sheet can be found in the appendices to the School Online Safety Template Policies)
- These records will be reviewed by ... (Online Safety Officer / Online Safety Committee / Online Safety Governor) at regular intervals (state the frequency).
- This policy will be reviewed by the Headteacher and governors annually and in response to changes in guidance and evidence gained from the records.

A12 Mobile Technologies Policy

A12.1 Introduction

A12.1.1 Mobile technology devices may be a 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.

A12.1.2 All users should understand that the primary purpose of the use of school-owned/personal devices in a school context is educational.

A12.2 General Statements

A12.2.1 The school Acceptable Use Agreements for staff, pupils/students and parents/carers will give consideration to the use of mobile technologies.

A12.2.2 The school allows:

	School-owned Devices			Personal Devices		
	School owned for single user	School owned for multiple users	Authorised device	Student owned	Staff owned	Visitor owned
Allowed in school	Yes	Yes	Yes	Yes[7]	Yes	Yes
Full network access	Yes	Yes	Yes	No	No	No
Internet only	Yes	Yes	Yes	No	No	Yes[8]
No network access				Yes	Yes	Yes

A12.3 School-owned Devices

A12.3.1 The school has provided technical solutions for the safe use of mobile technology for school-owned devices / personal devices:

- All school devices are controlled though the use of Mobile Device Management software
- Appropriate access control is applied to all mobile devices according to the requirements of the user (e.g Internet only access, network access allowed, shared folder network access)
- The school has addressed broadband performance and capacity to ensure that core educational and administrative activities are not negatively affected by the increase in the number of connected devices
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted

[7] Pupils bringing mobile/smartphones into school must have them turned off/silent and put away and not used in school.
[8] Secure "Guest wifi" is available for visitors/contractors' devices to enable them to carry out online work required as part of their visit. Staff/pupil personal devices will NOT be provided guest wifi access; school-owned devices are issued where staff require wifi access.

- Appropriate exit processes are implemented for devices no longer used at a school location or by an authorised user. These include; revoking the link between MDM software and the device, removing proxy settings, ensuring no sensitive data is removed from the network, uninstalling school-licenced software etc.
- All school devices are subject to routine monitoring
- Pro-active monitoring has been implemented to monitor activity

A12.4 Personal Devices

A12.4.1 When personal devices are permitted:

- Secure "Guest wifi" is available for visitors/contractors' devices to enable them to carry out online work required as part of their visit. Staff/pupil personal devices will NOT be provided guest wifi access; school-owned devices are issued where staff require wifi access.
- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network/wifi access
- Personal devices are brought into the school entirely at the risk of the owner and the decision to bring the device in to the school lies with the user (and their parents/carers) as does the liability for any loss or damage resulting from the use of the device in school
- The school accepts no responsibility or liability in respect of lost, stolen or damaged devices while at school or on activities organised or undertaken by the school (the school recommends insurance is purchased to cover that device whilst out of the home)
- The school accepts no responsibility for any malfunction of a device due to changes made to the device while on the school network or whilst resolving any connectivity issues
- The school recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the school. Pass-codes or PINs should be set on personal devices to aid security
- The school is not responsible for the day to day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- Monitoring records will be retained of resources that personal devices have accessed via the internet. However, personal devices will NOT be subject to enhanced monitoring, for example, through PCE.

A12.5 Additional Terms of Use

A12.5.1 Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition;

- Pupils are required to follow staff instruction with regard to when devices are permitted / not permitted to be used
- Devices may not be used in tests or exams
- Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
- Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
- Users are responsible for charging their own devices and for protecting and looking after their devices while in school
- Devices must be in silent mode on the school site and on school buses

- School devices are provided to support learning. It is expected that pupils and staff will bring school devices to school as required.
- Confiscation and searching (England) - the school has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
- The changing of settings (exceptions include personal settings such as font size, brightness, etc…) that would stop the device working as it was originally set up and intended to work is not permitted
- The software / apps originally installed by the school must remain on the school owned device in usable condition and be easily accessible at all times.
- The school will ensure that school devices contain the necessary apps for school work. Apps added by the school will remain the property of the school and will not be accessible to students on authorised devices once they leave the school roll. Any apps bought by the user on their own account will remain theirs.
- Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use.
- Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity, using school-owned equipment. All unnecessary images or videos will be deleted immediately.
- Staff owned devices should not be used for personal purposes.
- Printing from personal devices will not be possible.

A13 Social Media Policy

A13.1 Introduction

Social media is a broad term for any kind of online platform which enables people to directly interact with each other. However some games, for example Minecraft, World of Warcraft or Fortnite, and content sharing platforms such as You Tube, Pinterest and Twitter have social media elements to them.

The school recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and pupils may find creative ways to use social media. However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying, personal reputation and school reputation. This policy aims to clarify rules around the safe use of social media by the school, its staff, parents, carers and children.

A13.2 Scope

This policy is subject to the school's Codes of Conduct and Acceptable Use Agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the school
- Applies to such online communications posted at any time and from anywhere
- Encourages the safe and responsible use of social media through training and education
- Defines the monitoring of public social media activity pertaining to the school.

The school respects privacy and understands that staff and pupils may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the school's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a school account or using the school name. All professional communications are within the scope of this policy.

Personal communications are those made via 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.

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

Digital communications with pupils are also considered. Staff must not use social media to communicate with learners via a personal social media account for any purpose, including teaching and learning. This also applies if staff employment ceases.

A13.3 Roles & Responsibilities

A13.3.1 Leadership Team:

- Facilitating training and guidance on Social Media use
- Developing and implementing the Social Media policy
- Taking a lead role in investigating any reported incident
- Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
- Receive completed applications for Social Media accounts

- Approve account creation.

A13.3.2 Administrator / Moderator

- Create the account following Leadership Team approval
- Store account details, including passwords securely
- Be involved in monitoring and contributing to the account
- Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

A13.3.3 Staff

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via school accounts
- Adding an appropriate disclaimer to personal accounts when naming the school

A13.4 Personal use

A13.4.1 Staff

- 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.
- Personal communications which do not refer to or impact upon the school are outside the scope of this policy.
- Where excessive personal use of social media in school is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.
- Staff should not engage in online discussion on personal matters relating to members of the school community, and no reference should be made in social media to pupils, parents / carers, staff. This also applies if staff employment ceases.
- Security settings on personal social media profiles should be regularly checked to minimise risk of loss of personal information.

A13.4.2 Pupils

- Staff are not permitted to follow or engage with current or prior pupils of the school on any personal social media network account. This also applies if staff employment ceases.
- The school's education programme should enable the pupils to be safe and responsible users of social media.
- Any offensive or inappropriate comments will be resolved by the use of the school's Behaviour Policy / Professional Learning Standards.

A13.4.3 Parents/Carers

- If parents/carers have access to a school learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use.
- The school has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website.

- In the event of any offensive or inappropriate comments being made, the school will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the school's complaints procedures.

A13.5 Professional Use

A13.5.1 Process for creating new accounts

Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the Leadership Team an application will be approved or rejected. In all cases, the Leadership Team must be satisfied that anyone running a social media account on behalf of the school has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the school, including volunteers or parents.

A13.5.2 Monitoring

School accounts must be monitored regularly and frequently (preferably 5 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a school social media account.

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

A13.5.3 Behaviour

The school requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies.

Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. School social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the school.

Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to school activity.

If a journalist makes contact about posts made using social media staff must consult Leadership Team before responding.

Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the school and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.

The use of social media by staff while at work may be monitored, in line with school policies. The school permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken

The school will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the school will deal with the matter internally. Where conduct is considered illegal, the school will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

A13.6 Legal considerations

Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing. Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

A13.7 Handling abuse

When acting on behalf of the school, handle offensive comments swiftly and with sensitivity.

If a conversation turns and becomes offensive or unacceptable, school users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken

If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed school protocols.

A13.8 Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

A13.9 Use of images

School use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

Permission to use any photos or video recordings should be sought in line with the school's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected.

Under no circumstances should staff share or upload student pictures online other than via school owned social media accounts

Staff should exercise their professional judgement about whether an image is appropriate to share on school social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any school list of children whose images must not be published.

If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

A13.10 Appendix

A13.10.1 Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Do not post information publicly that you wouldn't want employers, colleagues, pupils or parents to see
- Do not retaliate to, or personally engage with cyberbullying incidents
- Social media can blur the lines between your professional and private life. Don't use the school logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections - keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images - do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem

A13.10.2 Managing school social media accounts

- Check with a senior leader before publishing content that may have controversial implications for the school
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties
- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the school's reporting process
- Consider turning off tagging people in images where possible
- Don't make comments, post content or link to materials that will bring the school into disrepute
- Don't publish confidential, personal or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of school accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances