BEDFORD GIRLS' SCHOOL

E-Safety Policy

Reviewed: August 2023
Next review: August 2024
Reviewed by: Becky Hudson-Findley and Kamelia Johnson

Scope of the Policy

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

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of online-bullying or other 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 Positive Behaviour Policy (and Addendums) and the Discipline and Exclusions Policy.

The school will deal with such incidents within this policy and associated anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate online safety behaviour that take place out of school.

The school will monitor the impact of the policy using:

- Logs of reported incidents on iSAMS and/or MyConcern
- Monitoring logs of internet activity including attempts to visit blocked sites / filtering
- Surveys/questionnaires

Roles and Responsibilities

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. This will be carried out by the Governors on the Co Curricular and Pastoral Committee receiving regular information about online safety incidents and monitoring reports.

In practice much of the day-to-day responsibility for e-safety will be delegated to the Designated Safeguarding Lead.

The role will include:

- Regular monitoring of online safety incident logs
- Regular monitoring of filtering logs
- Reporting to relevant Governors

SLT

Responsibilities:

- The Headmistress has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day to day responsibility for online safety will be delegated to the Designated Safeguarding Lead.
- The Headmistress and (at least) another member of the SLT should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff and will be dealt with in the first instance as a low-level concern. (Refer to flow chart for responding to incidents of misuse within this policy)
- The Headmistress is responsible for ensuring that the Designated Safeguarding Lead, E-Safety Coordinator and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.
- The SLT will receive monitoring reports from the Designated Safeguarding Lead as appropriate.

DSL

Responsibilities will include:

- Takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for the school community
- Liaises with the Harpur Trust as relevant
- Liaises with the IT Manager
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Attends relevant meetings of Governors
- Reports regularly to the SLT

As Designated Safeguarding Lead they 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

E-Safety Coordinator

The Designated Safeguarding Lead and the Director for Digital Learning, Enterprise and Sustainability take the lead role of the E-Safety Coordinator

Responsibilities will include:

- To liaise with other staff within the school to assist them in their role
- Meets with members of the school community as necessary to support the development and implementation of school policy and practice
- Oversees and provides training and advice for the school community
- Provides support to parents in the understanding of e-safety, which may be in the format of workshops or lectures, including responding to concerns raised.

IT Support Team

Those with technical responsibilities are responsible for ensuring:

- That the school's technical infrastructure is secure and is not open to misuse or malicious attack
- That the school meets required online safety technical requirements, including those set out in the current statutory guidance *Keeping Children Safe in Education*, and any Harpur Trust online safety policy/guidance that may apply
- That users may only access the network and devices through a properly enforced password protection policy
- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they stay updated with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network, internet and digital technologies in school are regularly monitored in order that any misuse/attempted misuse can be reported to the Headmistress/SLT/DSL/Director for Digital Learning, Enterprise and Sustainability for investigation, action and/or sanction.
- That monitoring software and systems are implemented and updated as agreed in school policies.

Teaching and Support Staff

Are responsible for ensuring that:

- They have an up to date awareness of online safety matters and of the current school online safety policy practices and procedures
- They have read, understood this E-Safety Policy and Student Acceptable Use Agreement
- They report any suspected misuse or problem to the Headmistress/SLT/DSL/Director for Digital Learning, Enterprise and Sustainability for investigation/action/sanction
- All digital communications with students, parents/carers should be on a professional level only and only carried out using official school systems
- Online safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Student Acceptable Use Agreement (AUA)
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

- They monitor the use of the digital technologies, mobile devices, cameras, etc. in lessons and other school activities (where allowed) and implement current policies with regard to these devices
- In lessons where it is intended to research potentially sensitive content students are 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

Students

- Are responsible for using the school digital technology systems in accordance with the Student Acceptable Use Agreement
- Have a good understanding of research skills, the need to avoid plagiarism and uphold copyright regulations appropriate to their age and level of study
- Need to understand the importance of reporting abuse, misuse and access to inappropriate materials and how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras.
- Will be expected to know and understand policies on the taking/use of images and online-bullying
- Should understand 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 the membership of the school
- Will be encouraged to contribute to E-Safety Policies, for example, at Student Voice meetings
- Will sign the relevant Student Acceptable Use Agreement after discussion with their teachers

Parents/Carers

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way.

The school will take every opportunity to help parents understand these issues through:

- Parents evenings
- Newsletters
- Letters
- Website
- Social media
- Information about national/local online safety campaigns

Parents and carers will be encouraged to support the school in promoting good online safety practice, both at school and at home, and to follow guidelines on the appropriate use of:

- Digital and video images taken at school events
- Access to parents' sections of the website/Google Classroom and online student records
- Their children's personal devices in the school

Policy Statements

Education - Students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in online safety/digital literacy is therefore an essential part of the school's online safety provision. Children and young people need the help and support of the school to recognise and avoid online safety risks and build their resilience.

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum.

The online safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities and will be provided in the following ways:

- A planned online safety curriculum should be provided as part of PSHE 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
- Students should be taught in all lessons to be critically aware of the materials/content they access online and be guided to validate the accuracy of information
- Students should be taught to acknowledge the source of information used and to respect copyright when using material access on the internet
- Students should be supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making
- Students should be helped to understand the need for the Student Acceptable Use Agreement and encouraged to adopt safe and responsible use both within and outside school
- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- All students receive continuing digital citizenship lessons through the tutor group and PSHE curriculum. Issues of online safety are explored further and we invite the Police School Liaison Officer to further reinforce the importance of staying safe online.
- Where students are allowed to use technology in lessons, staff should promote appropriate use for learning.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff 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.

Education - Parents and Carers

Many parents and carers may have only a limited understanding of online safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of the children's online behaviours. Parents may underestimate how often children and young people come across potential harmful and inappropriate material on the internet and may be unsure about how to respond.

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

- Curriculum activities
- Letters, newsletters, website
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. Safer Internet Day
- Reference to relevant websites and publications

Education and Training - Staff and Volunteers

It is essential that all relevant staff receive online safety training and understand their responsibilities, as outlined in this policy.

Training will be offered as follows:

- Formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand the school E-Safety Policy and Student Acceptable Use Agreement.
- It is expected that some staff will identify online safety as a training need within the performance management process
- The Designated Safeguarding Lead and E-Safety Coordinator will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations
- The E-Safety Policy and its updates will be presented to and discussed by staff in staff meetings/training sessions
- The Designated Safeguarding Lead and E-Safety Coordinator will provide advice/guidance/training to individuals as required

Training - Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any 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 Harpur Trust, National Governors Association or other relevant organisation
- Participation in school training/information sessions for staff or parents

Technical - Infrastructure/Equipment, Filtering and Monitoring

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

Management of Technical Systems

- School technical systems will be managed in ways that ensure the school meets recommended technical requirements as outlined in Government guidance
- Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff
- There will be regular reviews and audits of the safety and security of school technical systems
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the school systems and data. These are tested regularly. The school infrastructure and individual devices are protected by up to date virus software, with the exception of iPad devices.
- Servers, wireless systems and cabling must be securely located and physical access restricted
- Mobile device security and management procedures are in place

- IT Manager or a designated member of IT Support Team 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 to ensure compliance with the Copyright Act

Management of Users and Access

- 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 the IT Manager who will keep an up to date record of users and their usernames. Users are responsible for the security of their username and password.
- There are multiple "master/administrators" with individual passwords for the school systems, used by the IT Manager (and other authorised persons) with no single point of failure.
- An agreed procedure is in place for the provision of temporary access of 'guests' (e.g. visitors, volunteers) and this access expires after use. Staff may request guest wifi access only for visitors to the IT Support team with minimum 24 hour notice. Wifi with network access to staff, supply teachers, trainee teachers and visitors will only be provided following HR approval.
- An agreed policy is in place that forbids staff from downloading executable files and installing programs on school devices. Any attempt is blocked by the device. Approved software can be downloaded from the Software Centre or Self Service app.

Password Requirements

Passwords must:

- Be changed on first login to the system
- Be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack.
- Be minimum 10 characters, and include at least two of the following: an uppercase character, punctuation mark or number and will be rejected by systems at setup unless they meet this minimum criteria.
- Not include names, dates of birth or any personal information about the user that might be known by others.
- Be different for systems used inside and outside of the school.
- Be changed annually, or immediately if is believed the password is compromised

Management of Internet Access

- Internet access is filtered for all users. All explicit content is filtered. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet as school is responsible under the Counter Terrorism and Securities Act
- The school has provided enhanced/differentiated user-level filtering
- School technical staff regularly monitor and record the activity of users on the school technical systems and users are made aware of this in the acceptable use agreement
- Users report any actual/potential technical incident/security breach to the IT Manager and IT Team, in writing by emailing helpdesk@bedfordgirlsschool.co.uk

Mobile Technologies (Including BYOD)

Mobile technology devices may be school owned/provided or personally owned 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(s) 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 school context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant school policies including but not limited to the Safeguarding Policy, Positive Behaviour Policy (and Addendums), Anti-Bullying Policy, Acceptable Use Agreement and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the school's online safety education programme.

The school Student Acceptable Use Agreement will give consideration for the use of mobile technologies.

The school allows:

Device Type	Owner	Allowed in school	Network access	Internet Access
School Devices	School owned for single user	Yes	Yes	Yes
	School owned for multiple users	Yes	Yes	Yes
	Authorised device *(see below)*	Yes	Yes	Yes
Personal Devices	Student owned	Yes	No	Yes
	Staff Owned	Yes	No	Yes
	Visitor Owned	Yes	No	Yes

An authorised device - purchased by the student/family through a school-organised scheme, such as a school managed iPad. This device may be given full access to the network as if it were owned by the school.

The school has provided technical solutions fo the safe use of mobile technology for the school devices:

- All school devices are controlled through 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. Broadband is provided by two 500Mb fibre internet connections via two different ISPs.
- For all mobile technologies, filtering will be applied to the internet connection and attempts to bypass this are not permitted
- 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, uninstalling school-licensed software and/or wiping the device as appropriate.
- All school devices are subject to routine and proactive monitoring

When personal devices are permitted:

- All personal devices are restricted through the implementation of technical solutions that provide appropriate levels of network 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. Passwords 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 personal devices such as the charging of any device, the installation of software updates of the resolution of hardware issues

Users are expected to act responsibly, safely and respectfully in line with current Acceptable Use Agreements, in addition:

- Devices may not be used in tests or exams (unless explicit permission granted by staff)
- 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 school issued devices and for protecting and looking after their devices while in the school
- Personal devices should be charged before being brought to the school as the charging of personal devices (including school issued iPad device) is not permitted during the school day
- Devices must be in silent mode on the school site and on school transport
- School devices are provided to support learning. It is expected that students will bring devices to the 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. From time to time the school may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have no removed required apps
- The school will ensure that 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. All unnecessary images or videos will be deleted immediately.
- Devices may be used in lessons in accordance with teacher direction.

Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet.

However, staff, parents/carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for online bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The school will inform and educate users about these risks and implement policies to reduce the likelihood of the potential for harm.

- When using digital images, staff should inform and educate students 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.
- In accordance with the Retention of Records Policy, written permission from parents or carers will be obtained before photographs of students are published within the school’s promotional material such as the prospectus, website and social media, or in the local press. This is obtained through the Parent Contract at admission. Where the student is of sufficient maturity (usually when aged 12 years or older), the school may seek the student’s specific prior consent in addition to or instead of the consent of parents or carers.
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images
- 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 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 should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other students in the digital/video images.
- 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 be taken on school equipment where possible.

    - Personal equipment of staff may be used if the digital/video images are to only be used for school purposes. It is the responsibility of the photographer and/or the owner of the device to be sure that they are taken for the proper purpose and the data only held for the minimum time.
    - The data should be downloaded to school systems and used or deleted at the next reasonable opportunity in line with the Harpur Trust and school's Information Security Policies.
    - It is not reasonable for staff to collect photos on a personal device as personal memories;
    - Staff may be in breach of the Disciplinary Policy if inappropriate digital/video images are taken or stored on personal devices.
- Care should be taken when taking digital/video images that students are appropriately dressed and not participating in activities that might bring the individuals or the school into disrepute
- Students must not take, use, share, publish or distribute images of others without their permission
- Students' full names will not be used in association with photographs in the Junior School and may be used in the Senior School if appropriate.
- Students' work can only be published with the permission of the student and parents or carers, granted within the Parent Contract under Intellectual Property

Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The specific policies are detailed in the Data Protection Policies, which include:

- the implementation of the data protection principles and ability to demonstrate that the school does so through the use of policies, notices and records
- the holding of only the minimum personal data necessary to enable the school to perform its function and that it will not hold it for longer than necessary for the purposes it was collected for. The school has developed and implemented a Data Retention Policy to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this.
- Regular checks of IT system security. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring-fenced from systems accessible in the classroom/to learners.
- All staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any personal computer equipment, mobile device or removable media the:

- Data must be protected by up to date virus software and firewall
- Information relating to the school must not be saved onto the hard drive of personally owned devices
- Removable storage device must be protected from loss and/or theft using reasonable measures
- Data must be securely deleted from the device, in line with the school policy (below) once it has been transferred or its use is complete

Staff must ensure they:

- At all times take care to ensure the safekeeping of personal data, minimising the risk of its loss or misuse
- Can recognise a possible breach, understand the need for urgency and know who to report it to within the school
- Can help students (data subjects) understand their rights with respect to their data and know how to handle a request whether verbal or written. Know who to pass it to in the school
- Know where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected
- Will not transfer any school personal data to personal devices except as in line with school policy
- Access personal data sources and records only on secure password protected computers and other devices, ensuring that they are properly ‘logged off’ at the end of any session in which they are using personal data

Communications

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:

Communication Technologies	Staff & Other Adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to the school	x				x			
Use of mobile phones in lessons	x						x	
Use of mobile phones in social time	x					x		
Taking photos on mobile phones/cameras		x				x		
Use of BGS iPad device	x				x			
Use of other personal mobile devices e.g. tablets, gaming devices	x					x		
Use of school email for personal emails		x				x		
Use of video conferencing (Google Meet is the approved platform)	x						x[1]	
Use of messaging apps (Google Chat is the approved platform)	x					x		
Use of social media	x					x		
Use of blogs	x					x		

[1] Student accounts are configured to prevent students hosting Google Meet calls unless in Years 12 or 13. Students in Years 3 to 11 can only join Google Meets hosted by school staff.

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

- The official school email service **(@bedfordgirlsschool.co.uk** domain only) may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school systems (e.g. by remote access)
- 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 such communication
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or social media must not be used for these communications unless the need to do so is agreed with the Senior Leadership Team.
- Users should try to check their school email at least twice a day for new messages
- Students should be taught strategies to deal with inappropriate communications and be reminded on the need to communicate appropriate when using digital technologies
- Personal information should not be posted on the school website and only official email addresses should be used to identify members of staff

Social Media - Protecting Professional Identity

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

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

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

School staff should ensure that:

- They follow the Harpur Trust Social Media Policy and the school's Safeguarding policy.
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

When official school social media accounts are established there is:

- A process for approval, conducted by the Marketing Team
- Clear processes for the administration and monitoring of these accounts - involving at least two members of staff. The account credentials are held securely by the Marketing Team.

- A code of behaviour for users of the accounts is provided by the Marketing Team including
    - Systems for reporting and dealing with abuse and misuse
    - Understanding of how incidents may be dealt with under school disciplinary procedures

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the school or impacts 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
- The school permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to proactively monitor the internet for public postings about the school and this is undertaken by the Marketing Team
- The school should effectively respond to social media comments made by others according to a definite policy or process established by the Marketing Team

The school's use of social media for professional purposes will be checked regularly by the senior risk officer, Designated Safeguarding Lead or E-Safety Coordinator to ensure compliance with the school policies.

Dealing with Unsuitable/Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from school and all other technical systems. If such activity is considered a crime, it may be reported to the police. Other activities e.g. 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.

Prevent Strategy

As part of our duty to ensure that children and young adults are kept safe from terrorist and extremist material when accessing the internet, we apply a Filtering and Monitoring Procedure. This actively filters and blocks unsuitable and inappropriate material including potential unlawful terrorist and extremist materials. Details of the webblocker policies can be found on page 7 and page 4 of the appendix of the E Safety Filtering and Monitoring Procedure document: https://docs.google.com/document/d/1iodcs1HYIufkzuGvCVFfT57PIX8S8lyV/edit?usp=sharing&ouid=113258998585961998304&rtpof=true&sd=true

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

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images - the making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					x
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003					x
	Radicalisation, extremism and terrorism or any such materials that could be seen to draw/encourage individuals into terrorist activity					
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					x
	Criminally racist material in the UK - to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986.					x
	Pornography				x	
	Promotion of any kind of discrimination				x	
	Threatening behaviour, including promotion of physical violence or mental harm				x	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				x	
Activities that might be classed as cyber-crime under the Computer Misuse Act:	● Gaining unauthorised access to school networks, data and files, through the use of computers/devices ● Creating of propagating computer viruses or other harmful files ● Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) ● Disable/impair/disrupt network functionality through the use of computers/devices ● Using penetration testing equipment (without relevant permission)					x

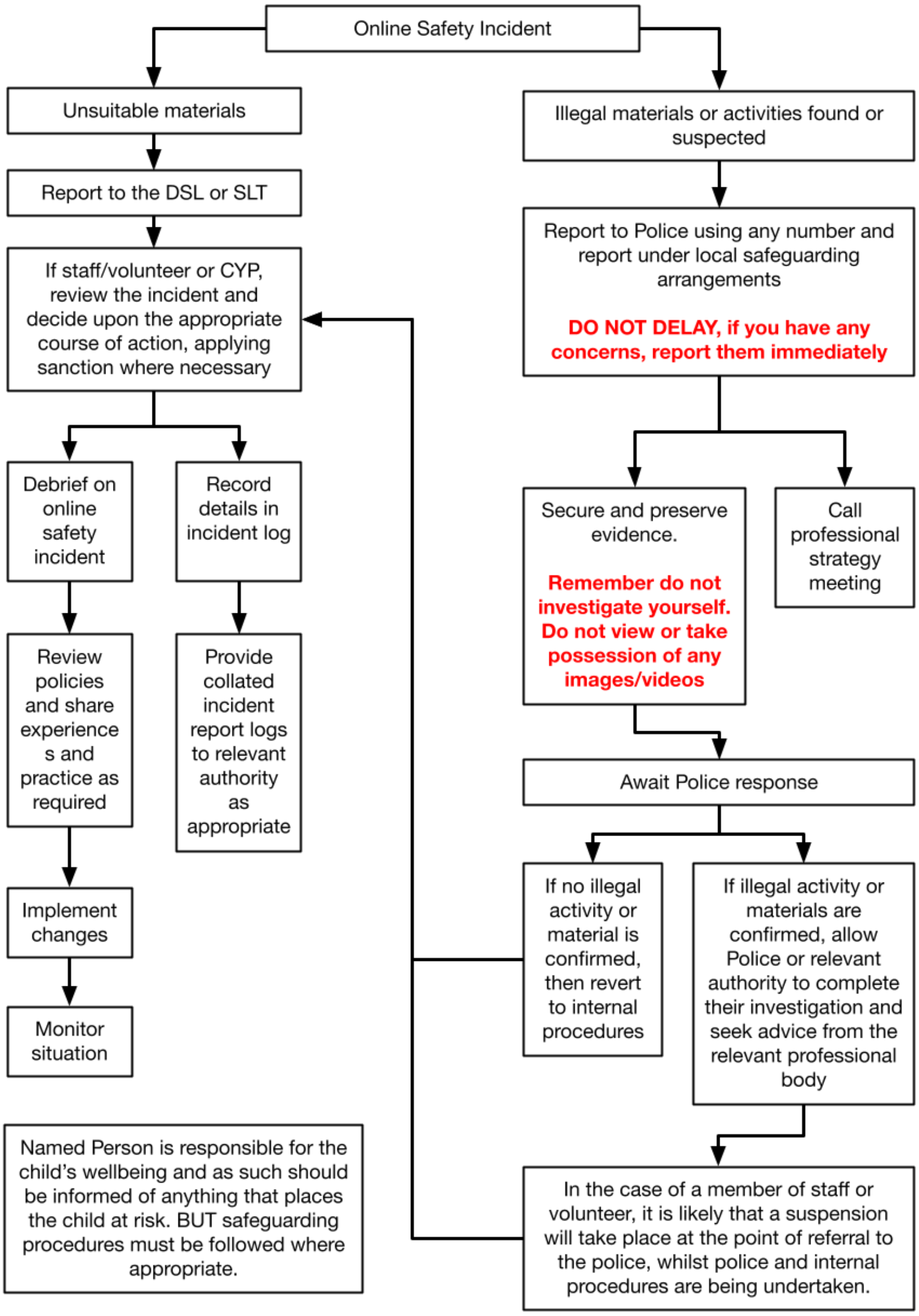
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the school				x	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				x	
Unfair usage (downloading/uploading large files that hinders others in their use of the internet)				x	
Using school systems to run a private business				x	
Infringing copyright				x	
Online gaming (educational)		x			
Online gaming (non-educational)				x	
Online gambling				x	
Online shopping/commerce		x			
File sharing (Google Drive is the approved platform)	x				
Use of social media		x			
Use of video conferencing (Google Meet is the approved platform)		x			
Use of messaging apps (Google Chat is the approved platform)		x			
Use of video broadcasting e.g. youtube		x			

Responding to Incidents of Misuse

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).

Illegal Incidents

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


Online Safety Incident
Unsuitable materials
Report to the DSL or SLT
If staff/volunteer or CYP, review the incident and decide upon the appropriate course of action, applying sanction where necessary
Debrief on online safety incident
Record details in incident log
Review policies and share experience s and practice as required
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child’s wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements
DO NOT DELAY, if you have any concerns, report them immediately
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to the police, whilst police and internal procedures are being undertaken.

Other Incidents

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 involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection)
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse - see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Involvement by the Harpur Trust or national/local organisation (as relevant)
    - Police involvement or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instance 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
    - Offences under the Computer Misuse Act (see User Actions chart above)
    - 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
- It is important that all the above steps are taken as they will provide an evidence trail for the school and possibly the police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the group for evidence and reference purposes.

School Actions and Sanctions

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:

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

Using proxy sites or other means to subvert the school’s security system		x	x			x	x	x	[x]
Accidentally accessing offensive or pornographic material and failing to report the incident		x	[x}	x	x	x		x	[x]
Deliberately accessing or trying to access offensive or pornographic material		x	x	x	x	x			x
Distribution of material that infringes the copyright of another person	x	x						x	x
Infringes the Data Protection Act (e.g. sharing personal information without permission)	x	x		[x]		x	[x]	x	[x]

NB: Where bracketed [x] denotes a possible outcome dependent on severity.

Staff Incidents	Refer to line manager	Refer to Headmistress	Refer to HR	Refer to police	Refer to technical support staff for action re filtering/security etc.	Warning	Suspension	Disciplinary Action
Attempted access material that could be considered illegal (see list in earlier section on unsuitable/inappropriate activities)		x	x	x	x	x	x	x
Inappropriate personal use of the internet/social media/personal email	x	[x]	x	x		x	x	x
Unauthorised/inappropriate downloading or uploading of files	x		x		x	x		
Allowing others to access school network by sharing username and passwords		x			x	x	x	x
Attempting to access or accessing the school network, using another person’s account		x	x		x	x	x	x
Careless use of personal data e.g. holding or transferring data in an insecure manner	x	[x]				x	x	x
Deliberate actions to breach data protection or network security rules		x	x		x		x	x
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software		x	x	x	x		x	x

Sending an email, text or message that is regarded as offensive, harassment or of a bullying nature		x	x	x			x	x
Using personal email/social networking/instant messaging/text messaging to carry out digital communications with students	x	x	x			x	x	x
Actions which could compromise the staff member's professional standing	x	x	[x]			x	x	x
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		x	x			x	x	x
Using proxy sites or other means to subvert the school's security system	x	[x]			x	x		
Accidentally accessing offensive or pornographic material and failing to report the incident	x	x				x	x	x
Deliberately accessing or trying to access offensive or pornographic material		x	x	x			x	x
Breaching copyright or licensing regulations	x				[x]	x	x	x
Continued infringements of the above, following previous warnings or sanctions		x	x	x			x	x

NB: Where bracketed [x] denotes a possible outcome dependent on severity.

Student Acceptable Use Agreement

School Policy

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

This acceptable use agreement is intended to ensure:

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

Student Acceptable Use Agreement

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

For my own personal safety:

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

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

- I understand that the school systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

- I will not use the school systems or devices for online gaming or online gambling, unless I have permission of a member of staff to do so.

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

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

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

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

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

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

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

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

I will take responsibility for my school iPad:

- I will use my iPad in ways that are appropriate, meet school expectations and are educational
- I will only use my own password and will not share it with others
- I will never loan my iPad to others
- I will take good care of my iPad and protect it by handling it appropriately
- I will never leave the iPad unattended
- I will keep food and beverages away from my iPad as they may cause damage to the device
- I will not place decorations (such as stickers, markers etc.) on the iPad, only on a cover
- I will ensure that my iPad has the approved cover that will protect the device while it is in my use
- I agree to maintain the iPad, cover and power cord in good working condition
- I will ensure my iPad battery is fully charged for the start of the school day, knowing I will not be able to charge it during the school day
- I will not disassemble any part of my iPad or attempt any repairs. In case of damage I will report this to the school and my parents immediately
- In case of theft I will report this to the school and to my parents immediately
- I will be responsible for all damage or loss caused by neglect and abuse
- I will contact IT Support as soon as I identify a problem with my iPad that affects my learning and school work
- I understand that my iPad is subject to inspection at any time, without notice, and remains the property of Bedford Girls’ School

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

Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Agreement; to which it is attached.

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

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

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

Name of student:
Form Group:
Signed:
Date:

Parent/Carer Countersignature

Name of parent/carer:
Signed:
Date: