Online Safety Policy

This policy should be read in conjunction with the following policies:

- AI Policy
- Anti-Bullying Strategy
- Behaviour Policies (Junior & Senior School)
- Concerns and Complaints Policy
- Harpur Trust Social Media Policy
- Harpur Trust General Data Protection Regulation (GDPR) Policy
- Harpur Trust Information Security Policy
- Harpur Trust Safeguarding Policy
- Health and Safety Policy
- ICT Acceptable Use Policy (ICT AUP)
- Safeguarding and Child Protection Policy
- Staff Email Protocol Document
- Staff Code of Conduct Policy

This policy should be read in conjunction with the following statutory guidance:

- DfE Cyber Security Standards for Schools and Colleges (2024)
- DfE Filtering and Monitoring Standards (2025)
- Keeping Children Safe in Education (2026)
- Relationships, Sex Education and Health Guidance (2025)
- Searching, screening and confiscation at school (2023)
- Sharing nudes and semi-nudes: advice for education settings working with children and young people (2024)
- Teaching online safety in school (2023)

All published school policies can be found on the school website here. Any other documentation listed can be requested via School Reception.

Introduction

This policy for all members of the school community, is implemented to protect the interests and safety of the whole school community. It aims to provide clear guidance on how to minimise risks and how to deal with any infringements.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism.
- **contact:** being subjected to harmful online interaction with other users; for example, peer to peer pressure, commercial advertising as well as adults posing as children or young adults; including through generative AI applications and chatbot technologies.
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images, including manipulated, synthetic or AI-generated images and videos,, or online bullying; and
- **commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams.

It is the duty of Bedford Modern School to ensure that every student and member of staff in its care is safe; and the same principles apply to the digital world as apply to the real world. IT and online communications provide unrivalled opportunities for enhanced learning in addition to traditional methods but also pose greater and more subtle risks to young people. Our students are therefore taught how to stay safe and legal in the online environment and how to mitigate risks, including but not limited to the risk of identity theft, bullying, harassment, grooming, stalking, radicalisation and abuse.

New technologies are continually enhancing communication, the sharing of information, learning, social interaction and leisure activities. Whilst exciting and beneficial both in and beyond the context of education, much IT, particularly online resources, are not consistently policed. Bedford Modern School recognises the rapid evolution of digital technologies and the new challenges they present to online safety. Innovations such as artificial intelligence (AI), deepfake media, augmented and virtual reality (AR/VR), and generative content platforms (e.g., ChatGPT, image generators) offer exciting educational opportunities but also introduce complex risks. These include misinformation, identity manipulation, immersive environments that may affect wellbeing, and the potential for exploitation through synthetic media. All users need to be aware of the range of risks associated with the use of these internet technologies and must read and sign the ICT AUP. Technology, and risks and harms related to it, evolve, and change rapidly. This policy is reviewed annually or sooner, should the need arise.

At Bedford Modern School, we understand the responsibility to educate our students on online safety issues; teaching them the appropriate behaviours and critical thinking skills necessary to enable them to remain both safe and within the law when using the internet and related technologies in and beyond the classroom.

Both this policy and the ICT AUP are available online and cover both fixed and mobile devices provided by the School as well as all devices owned by students and staff brought onto school premises. All users whether staff, governors, students or guests must read this policy and the ICT AUP prior to using their provided login details; upon their first login they must click/accept these policies. All parts of this Online Safety Policy and ICT AUP should be understood fully prior to acceptance and any questions that arise should be directed to the e-Safety Coordinator or the ICT Services and Innovations Manager.

Roles and responsibilities

The e-Safety Coordinator, Designated Safeguarding Lead and ICT Services and Innovations Manager have responsibility for ensuring this policy is upheld by all members of the School community and updated annually or when there is a concern, whichever is sooner. They will keep up to date on current online safety issues and guidance issued by organisations such as the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International and the Local Authority Safeguarding Children Board. Governors are kept informed with regards to online safety through the Deputy Head (Pastoral and Student Progress) reporting on Safeguarding in Education Sub Committees and full body Governor Meetings. As with all issues of safety at this school, staff are encouraged to create a talking culture in order to address any online safety issues which may arise in classrooms on a daily basis.

Bedford Modern School believes that it is essential for parents / carers to be fully involved with promoting online safety both in and outside of school. Newsletters/bulletins for staff and parents are distributed regularly and we consult and discuss online safety matters with parents, students and staff in order to promote a wide understanding of the benefits and risks related to internet usage.

Staff awareness

New staff receive information on Bedford Modern School's Online Safety Policy and ICT AUP as part of their induction. All staff receive regular information and training on online safety issues in the form of INSET training, safeguarding questions of the week. Staff are

made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety, online safety elements of KCSIE.

All staff working with students are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. These behaviours are summarised in the ICT AUP which must be signed and returned before use of technologies in school. When students use school computers, staff should make sure they are fully aware of the agreement they are making to follow the School's IT guidelines.

Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the School community.

All staff should be aware that technology is a significant component in many safeguarding and wellbeing issues. Students are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Students can also abuse their peers online, and the sharing of material or messages, to those who do not want to receive such content and the creation, sharing or possession of manipulated, synthetic or AI-generated intimate images.

In the event of an online safety incident occurring, it must be recorded on CPOMS (Child Protecting and Online Management System), alerting the Designated Safeguarding Lead, Assistant Head, Head of Year and e-Safety Coordinator. The Designated Safeguarding Lead and e-Safety Coordinator will then monitor trends across the School.

Online Safety in the curriculum and school community

IT and online resources are used increasingly across the curriculum. We believe it is essential for online safety guidance to be given to students on a regular and meaningful basis. We continually look for new opportunities to promote online safety and regularly discuss our students' understanding of it through PSHE/RSE and selected student groups.

The School provides opportunities to teach about online safety within a range of curriculum areas and IT lessons. Educating students on the dangers of technologies that may be encountered outside school will also be carried out via ICT, RSE lessons, year assemblies (internally and externally presented), PSHE/RSE lessons, common room display boards, Safer Internet Day, educational visits and informally when opportunities arise. Parent Programme evening sessions and Parent Information Hub termly publications provide information that covers key areas of online safety and occur regularly throughout the academic year.

At age-appropriate levels students are taught to look after their own online safety. In the Junior School, an online safety assembly is delivered annually to each year group during Safety Week, or sooner should the need arise. From time to time, a member of Bedfordshire Police Cyber Protect and Prevent Team or the Children and Young People Development Officer and School Co-ordinator for Bedfordshire Police also attends to deliver assemblies. In Year 7 all students attend Bletchley Park for a dedicated online safety trip. In Year 7 to 11, Online Safety is delivered through dedicated PSHE lessons. In Years 7 to 9 students complete five dedicated Online Safety lessons throughout the year in ICT, in these lessons they cover the eight strands identified in the Education for a Connected World document produced by the UK Council for Internet Safety. From Year 10, students are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. In Year 12 and 13, students have an assembly on online responsibilities and behaviours delivered by Bedfordshire Police Cyber Division. Students are taught about respecting other people's information and images etc. through assemblies, posters, PSHE discussion, Safer Internet Day and classroom activities. Students can report concerns to the e-Safety Coordinator and any member of staff at the School.

Students should be aware of the impact of cyber-bullying (and know how to seek help if they are affected by these issues (see also the School's Anti Bullying Policy). Students should approach the e-Safety Coordinator as well as parents, peers and other school staff for advice or help if they experience problems when using the internet and related technologies.

Students with Increased Risk of Vulnerability

Some students have increased risks of safeguarding concerns (identified in KCSIE). These students also have increased vulnerability online. With a talking culture in place, these students are encouraged to discuss any issues that they have with their Form Tutor, Head of Year, Assistant Head of Year or their Academic Support teacher. The Wellbeing Team also support. Should an online safety incident occur involving a SEND student, the DSL, Head of Year, e-Safety Coordinator and Academic Support Department will be consulted to ensure that the correct terminology is used in all online safety discussions with this student.

Further information and support

This list is not extensive but should provide a useful foundation:

www.ceop.police.uk/safety-centre/
www.childnet.com/
www.disrespectnobody.co.uk
www.gov.uk/government/publications/the-use-of-social-media-for-online-radicalisation
www.internetmatters.org
www.saferinternet.org.uk
www.thinkuknow.co.uk
www.nspcc.org.uk/preventing-abuse/keeping-children-safe/share-aware/
www.net-aware.org.uk/
www.parentzone.org.uk/
www.sharechecklist.gov.uk/
https://apwg.org/

Use of school and personal devices

Staff

School devices assigned to a member of staff as part of their role must have a unique username and password or device lock so that unauthorised people cannot access the content. When they are not using a device, whether school or personal, staff should ensure that it is locked to prevent unauthorised access.

Staff at Bedford Modern School are permitted to bring in personal devices for their own use. They may use their mobile telephone for personal use only during break-times, lunchtimes or when they are otherwise not teaching and not in the presence of students.

Personal telephone numbers may not be shared with students or parents/carers and staff should only contact a student or parent/carer using a personal telephone number for teaching and learning purposes (with permission of LT) or in an emergency situation. Individual Microsoft Teams calls (or similar) may only be made with appropriate training and the advanced permission of both LT and parents, and records are placed on CPOMS.

Students

School owned mobile devices that are available for student use are stored in locked containers; access is available during lessons via the member of staff supervising the lesson.

If students bring in internet enabled personal devices they should be kept switched off and not used for personal use during lessons or in toilets or changing rooms, and will remain the responsibility of the student in case of loss or damage.

In the Junior School, students with specific travel arrangements or prior arrangement with the Deputy Head Junior School should hand their phone in to Reception at the start of the day and collected as they leave school. Other students should not bring a phone into school.

Mobile phones or similar devices are not allowed in the refectory at lunchtime or when in the corridors and walking around the school site. Mobile phones should only be used in sixth form only areas or when specific permission has been provided by a member of staff.

Use of internet and email

The School is not able to monitor any Internet access or content accessed by a user using their own devices through non-school controlled wireless or network systems, such as mobile and emerging wireless communication technologies, 'Hotspots', Proxy or VPN bypass Systems. Where applicable, the school may however still be able to monitor Microsoft Team Chats initiated on a user's school account for the purposes of protecting users from any safeguarding issues/concerns.

Staff

Staff must use social networking sites with extreme caution, being aware of the nature of what is published online and its potential impact on their professional position. It is accepted that some sites may be used for professional purposes to highlight a personal profile with summarised details, e.g., LinkedIn. It is advised that this should be well maintained and kept up to date with a high level of presentation on such sites should Bedford Modern School be listed.

There are layered cyber security controls, filtering, endpoint protection, monitoring and authentication controls. Staff should be aware that email communications should be in line with the Email Protocols Document (within the staff handbook). Network activity is monitored, with specialist software, to reduce the risk of access to inappropriate material and protect their safety online.

Staff must immediately report the receipt of any communication that may be in breach of cybersecurity, makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature to the e-Safety Coordinator or ICT Services and Innovations Manager and must not respond to any such communication.

Any online communications must not either knowingly or recklessly:

- place a child or young person at risk of harm;
- bring Bedford Modern School into disrepute;
- breach confidentiality;
- breach copyright;
- breach data protection legislation;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
    - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, marriage or civil partnership, pregnancy/maternity, religion or belief or age;
    - using social media to bully another individual; or
    - posting links or material which is discriminatory or offensive.

Current students or parents should not be added as social network 'friends' unless staff have a pre-existing social relationship with them out of school.

Any digital communication between staff and fellow staff, students or parents / carers must be professional in tone and content. Staff should not contact a student or parent / carer using any personal email address unless under extenuating circumstances. The School ensures that staff have access to their work email address when offsite, for use as necessary on school business. Staff should not interact with students within a closed environment, e.g. texting from a phone, instant messaging, personal email, or within a

semi-closed environment e.g. writing on a 'wall' within Facebook or communicating with someone who 'protects' their updates on X. Online interaction within an 'open' online environment, for example standard X updates, may be appropriate, but still require professional judgment. If in doubt seek advice from the DSL or e-Safety Coordinator.

Students

All students are issued with their own personal school e-mail addresses for use on our network and by remote access. Access is via a personal login, which is password protected. This official email service may be regarded as safe and secure and must be used for all schoolwork. Students should be aware that email communications are monitored, and the School monitor, with specialist software, user's network activity to reduce the risk of access to inappropriate material and protect their safety online.

There is strong anti-virus and firewall protection on our network. Spam emails and certain attachments will be blocked automatically by the email system. If this causes problems for schoolwork, students should contact the ICT Services Team for assistance.

Students should immediately report the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature to their Form Tutor and the e-Safety Coordinator or ICT Services and Innovations Manager and must not respond to or share any such communication.

Students must report any accidental access to materials of a violent or sexual nature directly to their Form Tutor, e-Safety Coordinator or ICT Services and Innovations Manager. Deliberate access to any inappropriate materials by a student will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour Policy (Junior & Senior School – Behaviour Policy). Students should be aware that all internet usage via the School's systems and its Wi-Fi network is monitored, and is a privilege and not a right.

Certain websites are automatically blocked by the School's filtering system. If this causes problems for schoolwork, students should contact their Form Tutor for assistance, who will submit a request for unblocking via two designated email addresses, for the Junior School and Senior School respectively.

Students may have unlimited and unrestricted access to the internet via mobile phone networks, mobile and emerging wireless communication technologies. This access means some students, whilst at School, may access harmful content. The School strongly recommends that student owned devices have adequate filters, updates and protection in place and to report any access to harmful content immediately.

Safe 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 cyberbullying, stalking or grooming 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.

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).

Staff are allowed to take digital / video images to support educational aims, but must follow this policy, the ICT AUP and Information Security Policy concerning the sharing, distribution and publication of those images. These images should only be taken strictly to support educational and co-curricular aims and must be taken on school equipment; personal equipment should not be used for such purposes without prior permission from a member

of LT. Should an image be taken on a personal device, if the aim of this image is short term, once achieved it must be deleted from the personal device including cloud storage. If the aim of this image is longer term it must be transferred to the school system and deleted from the personal device as promptly as possible.

Care should be taken when taking digital / video images that students are appropriately dressed and are 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 at school without their permission and are reminded to be wary of sharing images that may identify their location.

Photographs or images for use in promotional material are in line with the parental terms and conditions and comply with good practice guidance on the use of such images.

Complaints

Reasonable precautions have been made however as with all issues of safety at Bedford Modern School, if a member of staff, a student or a parent / carer has a complaint or concern relating to online safety prompt action will be taken to deal with it. Complaints should be addressed to the e-Safety Coordinator (and in their absence to the DSL); if the matter is strictly a staff matter it must be addressed to the SDH. In the first instance, an investigation will be completed, and the e-Safety Coordinator will liaise with any members of staff or students involved. More formal complaints should be handled in line with the Concerns and Complaints Policy.

References:

Child Safety Online: A practical guide for parents and carers 2016
https://www.getsafeonline.org/
Childnet International
UK Safer Internet Centre
The South West Grid for Learning
Child Exploitation and Online Protection Centre
http://swgfl.org.uk/
NSPCC
Education for a Connected World - GOV.UK (www.gov.uk)

Mr D Donoghue
e-Safety Co-ordinator

October 2026
Review Date October 2027