Online Safety Policy

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

- Safeguarding and Child Protection Policy
- Behaviour Policy (Junior & Senior School)
- Anti-Bullying Policy
- Health and Safety Policy
- ICT Acceptable Use Policy (ICT AUP)
- Staff Email Protocol Document
- Harpur Trust Social Media Policy
- Harpur Trust General Data Protection Regulation (GDPR) Policy
- Harpur Trust Information Security Policy
- Concerns and Complaints Policy
- Staff Code of Conduct Policy
- Relationships, Sex Education and Health Guidance
- Keeping Children Safe in Education 2020 (including Annex C)

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 three areas of risk:

- **content:** being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
- **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
- **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

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. Current and emerging technologies used in and outside of school include:

- Websites;
- Email and instant messaging;
- Blogs;
- Social networking sites;
- Chat rooms;
- Music / video downloads;

- Gaming sites;
- Text messaging and picture messaging;
- Video calls;
- Podcasting;
- Online communities via games consoles; and
- Mobile internet devices such as smart phones and tablets.

Whilst exciting and beneficial both in and beyond the context of education, much IT, particularly online resources, are not consistently policed. 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.

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. The Safeguarding Governor is consulted with regard to online safety. 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, regular Online Safety Newsletters/Bulletins and via a dedicated subfolder within the allstaff (S:\Online Safety). The aim of this folder is to highlight possible resources, topical articles, past assemblies and initiatives. Staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety, including Annex C: Online Safety of KCSIE 2020.

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 children 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.

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.

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, PSHE/RSE, year assemblies (internally and externally presented), common room display boards, Safer Internet Day, educational visits and informally when opportunities arise.

At age-appropriate levels students are taught to look after their own online safety. In the Junior School, the e-Safety co-ordinator delivers an assembly annually to each year group during Safety Week, or sooner should the need arise. From time to time 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 9 students complete a cybersecurity exercise in IT. 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, as part of their enrichment programme, students have an assembly on online responsibilities and behaviours delivered by Bedfordshire Police. Students are taught about respecting other people's information and images etc. through assemblies, posters, 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 (highlighted in anti-bullying week and anti-bullying boards in common rooms) 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 SEND

Students with SEND, at times, have an increased vulnerability to risk online, especially those with language and communication needs, or social communication difficulties. With a talking culture in place, our SEND students are encouraged to discuss any issues that they have with their Form Tutor, Head of Year, Assistant Head of Year or Support Teacher. Should an online safety incident occur involving a SEND student, the DSL, Head of Year, e-Safety Coordinator and SEND 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/

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.

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 or in common rooms via the member of staff supervising the lesson or duty.

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. They may be used in lessons for learning purposes if agreed by the member of staff.

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 school. Designated areas and times of use apply to each year group, information of which may be found in the School Rules which are set out in the Parent Information Booklet and in Essential Downloads on the website.

Use of internet and email

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 is strong anti-virus and firewall protection on our network and, as such, it may be regarded as safe and secure. Staff should be aware that email communications should be in line with the Email Protocols Document (within the staff handbook). Network activity may be 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 Twitter. Online interaction within an 'open' online environment, for example standard Twitter 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 may 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 the ICT Services Team for assistance.

Data storage

The school takes its compliance with GDPR seriously. Please refer to the Harpur Trust GDPR Policy, Harpur Trust Information Security Policy and ICT AUP for further details.

Staff and students are expected to keep data safe and secure, by saving their work on the School's central server or, where available, the Cloud, as per the ICT AUP.

Staff may only take information offsite when authorised to do so, and only when it is necessary and required in order to fulfil their role. If personal data of staff or students is needed to be stored on personal memory sticks, these must be encrypted before being taken off site after seeking advice from ICT staff.

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the ICT Services and Innovations Manager, ICT Services Team or the e-Safety Coordinator.

Password security

Students and staff have individual school network logins and storage folders on the server. Staff and students are regularly reminded of the need for password security.

All students and members of staff should:

- use a strong password (usually containing ten characters or more, and containing at least three of the following criteria: upper case letters, lower case letters, numbers or alphanumeric characters). You will be prompted to change this password annually;
- not write passwords down; and
- should not share passwords with other students, staff or guests.

Further detail on this can be found within the Harpur Trust Information Security Policy and/or the Bedford Modern School ICT AUP.

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

David Donoghue
e-Safety Co-ordinator

Interim Review February 2021
Review Date October 2021