Beths Grammar School

Online Safety Policy

This Online Safety policy will help support and protect children, young people and staff when using technology.

Why have an Online Safety Policy?

1. Use of new technology needs to be something we are building into our strategies to reach out and connect with young people. However, with every new release or update comes a new risk or element to be aware of. Never has it been so important for young people and for those of us who work with young people, to be kept safe online and in every other form of e-communication.

2. We should all welcome the development of new technologies for communicating and use them wherever they are appropriate to enhance our work within the school.

3. We need to recognise our responsibility to take all reasonable measures to ensure that the risks of harm to students' welfare are minimised; and, where there are concerns about students' welfare, to take appropriate actions to address those concerns.

4. Online Safety covers issues relating to children and young people and their safe use of the Internet, mobile phones and other electronic communication technologies, both in and out of school. It includes education on risks and responsibilities and is part of the **duty of care** which applies to everyone working with children.

5. We recognise the need to protect staff and volunteers from inappropriate conduct from young people in their personal lives and from situations that may make them vulnerable to allegations of wrongful conduct.

6. We acknowledge that working within the school requires appropriate conduct in public spaces outside our work and in our personal lives and that this includes electronic communications.

7. We will ensure that our staff and volunteers follow the requirements of all relevant legislation as well as the school's Safeguarding and Child Protection Policy.

8. The school's **Online Safety Officer** is the school's **Designated Safeguarding Lead (DSL)**. The DSL can be contacted via a phone call to the school's reception staff or via email to safeguarding@beths.bexley.sch.uk. See the school's Safeguarding and Child Protection Policy for details of the Safeguarding Officer.

Electronic Communication

9. Electronic communication includes using mobile phones, computers and other devices for e-mail, text, instant messaging, and social networking.

10. We will train our staff and volunteers to follow this policy and we will carry out a full review of this policy annually.

11. Under ordinary circumstances it is inappropriate to have private, non-work-related contact using electronic communication with students. However, we recognise that there will be times when it is necessary and important to use electronic communications, for example, sometimes it is easier for a student to express a concern, thought or question using an email rather than in person, or to use the Instant Messaging feature via Microsoft Teams.

12. We should not use electronic communication for general socialising or unnecessary contact. When a member of staff or volunteer is a relation of the student or a close family friend, they must take care to follow the spirit of this policy.

13. Appropriate reasons for contact could include responding to a question or comment from a young person, contacting them to reassure them of support or confirming arrangements for a school activity.

14. Unnecessary contact could include sharing personal issues or anything that might burden a young person. Excessive contact will also be inappropriate. Staff and volunteers should make their line manager or team leader aware when they are using electronic communication with a young person for any extended reason.

15. Parents/Carers are responsible for monitoring their children's electronic communication, social media and on-line activities. We will explain our policies and practice to parents and carers and seek to ensure they are aware that we use electronic communication as part of our work with students.

16. Unless a student is at risk or there are extenuating circumstances, we will observe a parent or carer's wish that we do not use electronic communication to contact a student.

17. All users must adhere to the generally accepted rules of network etiquette (netiquette). These include but are not limited to the following:

    - Be polite.
    - Use appropriate language.
    - Do not use abusive language in your messages to others.
    - Do not reveal the address, phone number or other personal details of yourself or other users.
    - Do not use the network in such a way that would disrupt the use of the network by other users.
    - Note that email is not guaranteed to be private.
    - Know that system administrators monitor and can access all mailboxes.
    - Never share passwords with others.

Mobile phones and texting

18. Staff and volunteers should not give or use their private mobile phone number to any student unless they have agreed this with their line manager or a Senior Leadership Team (SLT) member that it is appropriate to do so.

Safe Use of E-mail

19. Staff and volunteers should only use an agreed email account for email contact with any student, which will normally be an account set up specifically for this purpose i.e., a school e-mail account.

20. Staff and volunteers must not use their personal email account for any contact with a student. All students have now been issued with their own school email accounts, so these, along with Microsoft Teams, should be the preferred methods of communications. As with other forms of electronic contact, when a member of staff or volunteer is a relation of the student or a close family friend, they must take care to follow the spirit of this policy.

21. Staff and volunteers should take great care not to use language that might give the wrong impression or create misunderstanding when communicating with a student, especially when using the informal language and shorthand often used in texts. Staff and volunteers should seek advice from a line manager or team leader whenever there is doubt or concern over the content or context of electronic communication.

22. A record of emails sent and received should be backed up electronically for reference and made available to a line manager or team leader if required.

- E-mail/Microsoft Teams is now an essential means of communication for staff (and increasingly for students). Directed e-mail use alongside Microsoft Teams, can bring significant educational benefits through increased ease of communication.

- If a member of staff (or student) receives an e-mail that is considered disturbing or inappropriate it should be reported to the **Online Safety officer**.

- Staff or students should never respond to malicious or threatening messages but should report them as soon as possible to the **Designated safeguarding lead**.

- The school will investigate any relevant inappropriate e-mails sent to staff or students.

- The school electronically filters e-mail to exclude spam e-mail or the use of inappropriate language, wherever possible.

- Staff should consider other means of contact with students i.e., Teams/Show My Homework.

- Staff e-mail addresses (issued by the school) must be provided by staff to students when there is a need of email contact for educational purposes. Staff can also use Microsoft Teams for more direct communications.

- Staff must use the school e-mail system for professional purposes **only** and always use professional language.

- Staff should not give students their **personal** e-mail addresses.

- Staff accessing e-mail via their handheld devices must ensure that personal and sensitive information is not visible to a third party. Confidential and sensitive information should not be accessed in a public place. Staff should also make full use of any security features of their devices for securing access.

Social networking and instant messaging

23. Unlike email or texting, social networking and instant messaging involves the possibility of contact with the friends of the student or of the staff member or volunteer. This raises concerns for safeguarding young people.

24. Staff should be aware that as public figures, they are under scrutiny over their activities both inside, and outside, the work environment. Any use of digital technologies which bring the member of staff or the school into disrepute could result in disciplinary action. Such digital technologies include, but is not limited to, use of social media sites, e-mail communication, blogs, digital images etc.

25. Staff and volunteers must only use an agreed social networking or instant messaging account for contact with young people with whom the school is working, which will normally be an account set up specifically for this purpose on behalf of a group rather than an individual.

26. Staff and volunteers must not use their personal social networking or instant messaging accounts for contact with students.

27. If a staff member or volunteer is contacted by a student on a social networking site, e.g., Facebook, WhatsApp, Snapchat etc. they must not respond by messaging that young person, even to inform them that contact in this way is prohibited since doing so will open the staff member's profile for the young person for one month. Instead, the matter should instead be followed up in person at the next appropriate opportunity.

28. Staff and volunteers must ensure that the content of their social networking accounts, including pictures, are appropriate. Comments and other content must not be derogatory towards the school or those with whom the school is working, including students, school staff and other organisations. Applications, groups and other content must be appropriate to the role of a staff member of the school and the ethos of the school. Privacy settings, where available; must be set at the highest levels.

Mobile phones and Handheld Devices

30. KS3 students are not permitted to use their mobile phones freely when on the school site, however on rare occasions, with the permission of a supervising teacher (or adult) students are permitted to use mobile phones in some lessons. KS4 and KS5 students have specific 'phone zones' where mobile phone use is permitted. Nevertheless, whether the device is a laptop, tablet or smart phone, risks must be appropriately assessed. The Wi-Fi provided for all student access is appropriately filtered, the same as the filtering applied to student desktop machines.

31. Due to an increase in the availability of 4G/5G networks coupled with an increase in "unlimited" data plans from mobile carriers; many students now have greater mobile Internet usage. This means that they cannot be filtered in accordance with the school's filtering policy. Staff must be aware of this and any other classroom management issues arising from use of this type of equipment.

32. It should also be recognised that the enhanced functionality of many handheld devices can be a cause for concern; and this should be considered a high risk in terms of potential misuse. Examples include the taking and distribution of indecent images or sexting, up-skirting (which is now a criminal offence), exploitation and bullying. Such abuse will have a negative impact on an individual's safety, dignity, privacy and right to confidentiality. Such concerns are not to be considered exclusive to students, so the needs and vulnerabilities of all must be respected and protected. Staff must be vigilant. They should challenge students and, if they deem it necessary, confiscate the handheld device, keep it safely and return it at an appropriate time, to the parent/carer if necessary.

33. Security is another issue. Students should be reminded to always keep their mobile devices with them. For Health and Safety reasons, the school will also not allow student devices to be connected to the mains supply for recharging. Students should also be reminded of this.

Disclaimer: Beths Grammar School accepts no liability in respect of any loss/damage to personal ICT equipment while at school or during school-sponsored activities. The decision to bring a personal ICT device into school rests with the student and their parent(s)/carer(s), as does the liability for any loss/damage that may result from the use of personal ICT equipment in school. It is a condition of agreeing to allow students to bring personal ICT devices into school, that the parent/carer accepts this disclaimer.

Wi-Fi Use

34. It is important that all members of the school community are fully aware of the school's boundaries and requirements when using the school's Wi-Fi system and take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse, and theft. This is not an exhaustive list, and all members of the school community are reminded that ICT usage should be consistent with the school ethos, other appropriate policies, and the law.

35. Please be aware that the school will not be liable for any damages or claims of any kind arising from the use of the wireless service. The school takes no responsibility for the security, safety, theft, insurance, and ownership of any device used within the school premises that is not the property of the school.

The Internet and on-line safety

36. Keeping Children Safe in Education (KCSIE 2023) includes clear references to online safety as part of a school's wider safeguarding strategy. It is important to remember that teachers and other staff members are also at risk and that the issues covered in this policy apply to them also.

What are the main threats and risks?

Online bullying

37. There is a great deal of pressure on young people today to succeed, to have the right kind of image, to be well-liked by others. The internet has been a very positive influence over this at times, providing advice, community, and enjoyment, acting as a stage for children and young people to express themselves and find a voice. However, at the same time, it can also be harmful to children who may find themselves falling victim to online bullying or harassment, whether by peers or anonymous sources.

38. Online bullying is most frequently seen through social media sites but can also be found on sharing websites or message boards. Behaviour can include malicious and insulting posts made anonymously or otherwise, sharing upsetting content directed at a particular individual, or posting unwanted photos to a wider network of peers.

39. It is important to remember that those who engage in bullying, whether online or offline, may have experienced the same treatment themselves. When dealing with incidents, it is crucial to consider the wellbeing of all the students involved, ensuring that any deeper issues are addressed in the process. Complaints of on-line bullying are dealt with in accordance with our Anti-Bullying Policy.

Online 'Self-baiting' and 'Self-harm'

40. The term ‘self-harm’ is generally defined by physical injuries that are auto inflicted, including cutting, over or under-eating and substance abuse.

41. The internet, however, has given rise to a new form of self-abuse, conducted predominantly through social media sites to inflict emotional or psychological harm. This can manifest in two ways:

    - ‘Self-baiting’ is where the victim posts an inflammatory comment to an online community in pursuit of inciting aggressive responses towards themselves.
    - ‘Online self-harm’ is where the victim creates false social media profiles to send offensive or insulting messages to their main profile, simulating third-party abuse.

    Both forms are used to effectively reinforce the negative feelings the victims have about themselves and validate their low self-esteem or personal image.

42. Action that should be taken to tackle internet issues such as bullying and self-harm includes:

    - Spotting and flagging up underlying issues in any case of self-harm, even online, and reporting these to the **Designated Safeguarding Lead**.
    - Knowing the environment - understanding what is available online and where the risks are is vital to safeguarding.
    - Ensuring students are aware of the value of a positive digital reputation and how to keep themselves safe through critical evaluation.
    - Taking every report of online bullying seriously, even if it is suspected to be self-inflicted - this may be a cry for help.
    - Working collaboratively - ensure that your reporting routes are accessible to everyone: staff, students, and parents/carers.

- Taking advantage of technology to help monitor and report online safety issues to the Safeguarding Officer if taking place within School systems.

Online Extremism and Radicalisation

43. Since the **Counter Terrorism and Security Act 2015** has come into effect, schools now have a duty of care to prevent people from being drawn into terrorism including online recruitment. There are several ways that online safety can be addressed to ensure that extremism and radicalisation do not pose a threat to the students. In addition to the education of students in this area (PSHCE, assemblies, talks etc), we have IT systems in place to reduce as far as possible students being exposed to extremism/on-line recruitment.

44. We have implemented two separate systems, or layers of security for our Internet. The first is provided by our Palo Alto firewall which has now taken on the role of filtering previously performed by Clearswift; the second by our internal system provided by Impero, which actively monitors student typed input for specific keywords. Impero have a set of keywords that are automatically flagged such as inappropriate language, but the school also uses custom keywords for any specific areas of concern that have been highlighted.

45. Staff or students who have any concern about themselves or others relating to on-line extremism or radicalisation should speak to the school's **Safeguarding Officer**.

<u>Other school policies relevant to the Online Safety policy</u>

- IT Acceptable Use policy (students)
- IT Acceptable Use policy (staff)
- Behaviour and Rewards policy
- Safeguarding and Child Protection policy
- Anti-Bullying policy
- Data Protection policy.

Reviewed Summer 2024
Next scheduled review date Summer 2025