E-SAFETY POLICY & PROCEDURE

Approving Body	Trust
Date of Last Review	December 2023
Statutory (Y/N)	Y
Responsible Officer	BMAT CEO for and on behalf of the Trust

I. AIMS, LEGISLATION AND ROLES OR RESPONSIBILITIES

1. **This Policy is a key part of BMAT's work to ensure that it:**
    a. Has robust processes to ensure the online safety of students, staff, volunteers, visitors, governors and trustees;
    b. Effectively educates the BMAT community in the safe use of technology; and
    c. Implements clear procedures to identify, intervene and escalate incidents, as appropriate.
2. **This Policy was drafted in line with:**
    a. Current legislation, including the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010.
    b. The Education Act 2011, which gives schools stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate content on students' electronic devices where there is a "good reason" to do so.
    c. Keeping Children Safe in Education (DfE)
    d. Advice from the DfE about Teaching Online Safety in Schools, "Preventing and Tackling Bullying and Cyber-Bullying, Relationships and Sex Education", Searching, Screening and Confiscation, and Preventing Radicalisation.
    e. BMAT's funding agreement and articles of association.
    f. The National Curriculum, as appropriate.
3. **Roles and responsibilities:**
    a. The Board of Trustees and Local Governing Bodies are responsible for overseeing the implementation of this Policy and for holding relevant BMAT staff to account for online safety, as appropriate.
    b. BMAT School Principals and co-headteachers are responsible for ensuring that this Policy is implemented consistently and effectively at a school level.
    c. Designated Safeguarding Leads (DSL) have lead responsibility for online safety in school. Among other things, they are required to deliver training about online safety, manage incidents of cyber-bullying and cooperate with school principals, Co-headteachers and external agencies, as appropriate. For more detail, see the BMAT Child Protection and Safeguarding Policy.
    d. ICT and/or Data Managers are responsible for ensuring that ICT systems are secure, regularly checked and updated, and appropriately filtered.
    e. All BMAT staff are required to understand this Policy and implement it consistently.

f. Parents or carers of BMAT students are expected to ensure that their child has read and understood this Policy.

g. Visitors who use BMAT ICT systems should be directed to this Policy.

4. Parents can seek further guidance on keeping children safe online from the following organisations and websites:
    a. What are the issues? - UK Safer Internet Centre.
    b. Hot topics - Childnet International.
    c. Parent factsheet - Childnet International.
5. This Policy is linked to our:
    a. Child protection and Safeguarding Policy;
    b. Information and Communication Technology Policy;
    c. Data Protection Policy;
    d. Student Behaviour Policy;
    e. Employee Disciplinary Policy;
    f. Complaints Policy.

II. EDUCATING STUDENTS ABOUT ONLINE SAFETY

1. The safe use of the internet and social media is covered in form time, assemblies and relevant subjects (e.g. PSHE and ICT).
2. The unsafe use of the internet and social media (e.g. cyber-bullying) will be dealt with in line with the BMAT Child Protection and Safeguarding Policy and the BMAT Student Behaviour Policy.
3. From September 2020, BMAT students will be taught about online safety as part of the National Curriculum. Online safety will be taught as part of Relationships and Sex Education and Health Education (RSE). A summary of the requirements is set out at Appendix A to this Policy.
4. BMAT have an RSE policy, which is published on the school websites. This Policy is made available to parents or carers, and letters will be sent home about the safe use of the internet and social media, as appropriate.
5. If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the heads of year, Headteacher/Principal, co-headteachers and/or the DSL.
6. Concerns or queries about this policy can be raised with any member of staff or the Headteacher/Principal/Co-headteachers.

III. CYBER-BULLYING.

7. **Cyber-bullying** is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.
8. **The most common places where cyberbullying occurs are:**
    a. Social Media, such as Instagram, Snapchat, TikTok, WhatsApp, Facebook, and Twitter;
    b. Text Messages sent through devices – whether as 'text messages' or on a specific app (e.g. WhatsApp or Messenger);
    c. Instant Message (via devices, email provider services, apps, and social media messaging features); and
    d. Email
9. **Special Concerns.** With the prevalence of social media and digital forums, comments, photos, posts, and content shared by individuals can often be viewed by strangers. The content an individual shares online – both their personal content as well as any negative, mean, or hurtful content – creates a kind of permanent public record of their views, activities, and behaviour. This public record can be thought of as an online reputation, which may be accessible to schools, employers, colleges, clubs, and others who may be researching an individual now or in the future. Cyberbullying can harm the online reputations of everyone involved – not just the person being bullied, but those doing the bullying or participating in it. Cyberbullying has unique concerns in that it can be:
    a. **Persistent –** Digital devices offer an ability to immediately and continuously communicate 24 hours a day, so it can be difficult for children experiencing cyberbullying to find relief.
    b. **Permanent –** Most information communicated electronically is permanent and public, if not reported and removed. A negative online reputation, including for those who bully, can impact college admissions, employment, and other areas of life.

c. **Hard to Notice –** Because teachers and parents/carers may not overhear or see cyberbullying taking place, it is harder to recognise.

10. **Preventing and addressing cyber-bullying.**
    a. BMAT will ensure that BMAT students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. For more information, see the BMAT Student Behaviour Policy, which includes our Code of Conduct.
    b. BMAT will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. These discussions will take place in form groups, assemblies, subject lessons and one-to-one or small group meetings, as appropriate.
    c. BMAT teaching staff are encouraged to use aspects of the curriculum to cover cyber-bullying, particularly the PSHE curriculum.
    d. Cyber-bullying is covered as part of the safeguarding training that is delivered to all BMAT staff. For more information, see the BMAT Child Protection and Safeguarding Policy.
    e. Incidents of cyber-bullying will be handled in line with the BMAT Student Behaviour Policy. Where illegal, inappropriate or harmful material has been circulated, BMAT will use all reasonable endeavours to ensure the incident is contained. The DSL and/or School Principal/Co-headteachers will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.
    f. Behaviour and safeguarding issues relating to cyber-bullying will be logged, as appropriate. Safeguarding issues will be logged by the DSL.

IV. EXAMINING ELECTRONIC DEVICES.

11. Under the Education and Inspections Act 2006 and the Education Act 2011, BMAT school staff have the power to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a "good reason'" to do so.
12. When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

a. Cause harm, and/or
b. Disrupt teaching, and/or
c. Break any of the school rules

13. If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:
    a. Delete that material; or
    b. Keep it as evidence; and/or
    c. Report it to the police.
14. Any searching of students will be carried out in line with the DfE's guidance on searching, screening and confiscation; and with the Section VII of the BMAT Student Behaviour Policy.
15. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the BMAT Complaints Policy.

V. ACCEPTABLE USE

16. Refer to the BMAT Information and Communication Technology (ICT) Policy for more information on BMAT's ICT systems and network, including access, appropriate use and responsibilities.
17. BMAT internet is to be used for educational purposes only, or for the purposes of fulfilling the duties of an individual's role.
18. BMAT monitors the websites visited by students, employees, volunteers, governors and visitors, to ensure they are acceptable.
19. BMAT employees are required to read and sign the BMAT Employee Code of Conduct, which includes a section on the responsible use of technology (including mobile devices and the use of BMAT ICT equipment outside of school premises).
20. Visitors and volunteers will be asked to read and agree to BMAT's terms on acceptable use, if appropriate.

VI. MOBILE DEVICES

21. "Mobile Device" means mobile phones, iPads or other tablets, laptops, smart watches, 'wearables' and any other devices which can connect to the internet/store data/take photographs.

22. BMAT accepts that mobile devices can be valuable for reasons of communication and personal safety. However, mobile devices can be a distraction from learning and used to cyber bully, misuse social media and to access or send inappropriate or unsafe content.
23. BMAT employees are required to:
    a. Lead by example, by not using personal mobile devices around students, unless it is for an agreed business purpose or because of an emergency; and
    b. Read and sign the BMAT Employee Code of Conduct, which includes a section on responsible technology use and mobile devices.
    c. Monitor the use of mobile devices by BMAT students, at all times, and to sanction inappropriate use in line with this Policy and the BMAT Student Behaviour Policy.
24. BMAT students are required to adhere to the following[1]:
    a. Mobile devices and headphones should not be seen or heard in school, unless a member of BMAT teaching staff has given express permission for students to use these devices for educational purposes;
    b. Sixth Formers may use mobile devices in the Sixth Form areas only.
    c. BMAT students are banned from using mobile devices during teaching time, including form group time and assemblies.
    d. BMAT students bring their mobile devices onto BMAT premises at their own risk and are responsible for their safe and secure storage.
    e. In line with its Security Policy, BMAT retains no liability for any mobile device that is brought onto its premises and lost, stolen, damaged or used in a manner which is against the owner's consent.

[1] Banning the use of mobile devices by students during teaching time is likely to improve the attainment rates and overall learning experience of BMAT students. "Ill Communication: The Impact of Mobile Phones on Student Performance" (LSE, 2015) shows that banning mobile devices from school premises:

a. Adds up to the equivalent of one week's schooling over each academic year;
b. Improves the test scores of students aged 16 by 6.4%;
c. Improves the test results of the lowest-achieving students by twice as much as average students; and
d. Has a greater positive impact on students with special educational needs and students eligible for free school meals.

f. Upon arrival at school and for the duration of any learning time (including form group time and assemblies), BMAT students are required to switch their mobile devices to "off", "do not disturb", "airplane mode" or "silent mode" and store them securely.

g. If BMAT students need to contact parents/carers or vice versa, during the school day, then that contact should be through school reception and not via mobile device.

VI. RESPONDING TO MISUSE

25. If a student misuses BMAT's ICT systems or internet, or a mobile device on BMAT premises, the matter will be dealt with in line with the BMAT Student Behaviour Policy.
26. Staff misuse will be dealt with in line with the BMAT Disciplinary Policy and Employee Code of Conduct.
27. All responses to misuse will be dealt with in line with the BMAT Data Protection Policy and with reference to the BMAT ICT Policy, as appropriate.
28. Action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
29. Behaviour and safeguarding issues relating to technology misuse will be logged, as appropriate. Safeguarding issues will be logged by the DSL.
30. Misuse of mobile devices:
    a. If any BMAT student uses a mobile device during teaching time, it will be confiscated, stored in a secure location on-site and returned to students by arrangement.
    b. If any BMAT student uses a mobile device for inappropriate purposes at any time during the school day and/or on BMAT premises (e.g. for cyber bullying, illicit recording or to access inappropriate material), their device will be confiscated, parents/carers should be contacted or called in for a meeting sanctions will be imposed, in line with the BMAT Student Behaviour Policy.
    c. Periods of confiscation may be extended to facilitate a proper investigation.
    d. Mobile devices will be passed onto external agencies, including the police, where appropriate.
    e. If a BMAT student refuses to hand over a mobile device to a member of BMAT staff, s/he will be issued with an appropriate sanction under the BMAT Student Behaviour Policy, and parents/carers should be contacted.

VII. TRAINING

31. All new BMAT employees receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.
32. All BMAT employees receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (e.g. emails, e-bulletins, meetings and Inset days).
33. DSLs and deputy DSLs receive more thorough and regular training, as set out in the BMAT Child Protection and Safeguarding Policy.
34. Trustees and governors receive training on safe internet use and online safeguarding issues as part of their safeguarding training.
35. Volunteers will receive appropriate training and updates, if applicable.

VIII. MONITORING

36. This Policy will be reviewed at least every three years, by the BMAT Trust Executive.

APPENDIX A – RSE REQUIREMENTS

1. BMAT students will be taught about online safety as part of the National Curriculum. Online safety will be taught as part of Relationships and Sex Education and Health Education (RSE). A summary of the requirements is set out below.
2. From September 2020, Key Stage Three students will be taught to:
    a. Understand how to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; and
    b. Recognise inappropriate content, contact and conduct, and how to report it.
3. From September 2020, Key Stage Four students will be taught to:
    a. To understand how changes in technology affect safety, including new ways to protect their online privacy and identity; and
    b. How to report a range of concerns.
4. From September 2020, by the end of secondary school, students will know:
    c. Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts.
    d. About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
    e. Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
    f. What to do and where to get support to report material or manage issues online.
    g. The impact of viewing harmful content.
    h. That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners.
    i. That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties.
    j. How information and data is generated, collected, shared and used online.
    k. How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviour.