



BABINGTON

HOUSE SCHOOL

ANTI-CYBER-BULLYING AND E SAFETY WHOLE SCHOOL (INCLUDING EYFS)

Babington House School

Date of Policy	Review Date	Reviewed By	Approved By
May 2026	May 2027 (unless new legislation comes in)	E Channon	SLT

Safeguarding and child protection are at the forefront and underpin all relevant aspects of process and policy development at Babington House School.
All systems, processes and policies operate with the best interests of the child at their heart.

IN THE CASE OF ANY SAFEGUARDING CONCERNS PLEASE CONTACT:

Elizabeth Channon echannon@babingtonhouse.com ext 255

Designated Safeguarding Lead

Jane Hawkins jhawkins@babingtonhouse.com DDSL

Kate Edwards kedwards@babingtonhouse.com ext 237

Deputy Designated Safeguarding Lead

David Laird dlaird@babingtonhouse.com DDSL

Gemma Bailey gbailey@babingtonhouse.com DDSL

RELATED POLICIES:

Anti-Bullying Policy

Data Protection Policy

Discipline and Behaviour Policy

Mobile Devices Policy

Pastoral Care Policy

Safeguarding Children Policy

Staff Code of Conduct

RELATED LEGISLATION / GUIDANCE

PREVENTING AND TACKLING BULLYING – JULY 2017

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/623895/Preventing_and_tackling_bullying_advice.pdf

CYBERBULLYING: ADVICE FOR HEADTEACHERS AND SCHOOL STAFF 2014

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/374850/Cyberbullying_Advice_for_Headteachers_and_School_Staff_121114.pdf

CHILDNET – USING TECHNOLOGY GUIDE

<https://www.childnet.com/teachers-and-professionals/for-you-as-a-professional/using-technology>

SAFER INTERNET FOR CHILDREN AND PARENTS

<https://www.saferinternet.org.uk/advice-centre/parents-and-carers/safety-tools-social-networks-and-other-online-services>

KEEPING CHILDREN SAFE IN EDUCATION 2026

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1181955/Keeping_children_safe_in_education_2023.pdf

WORKING TOGETHER TO SAFEGUARD CHILDREN 2026

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779401/Working_Together_to_Safeguard-Children.pdf

PREVENT DUTY GUIDANCE: ENGLAND AND WALES (2023)

<https://www.gov.uk/government/publications/prevent-duty-guidance>

SEARCHING, SCREENING and CONFISCATION (2022)

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1091132/Searching_Screening_and_Confiscation_guidance_July_2022.pdf

IF YOU HAVE CONCERNS ABOUT THE WELFARE OR SAFETY OF A PUPIL, PLEASE REFER IMMEDIATELY TO THE SAFEGUARDING POLICY AND FOLLOW THE PROCEDURES LISTED.

IF YOU HAVE CONCERNS RELATED TO PEER-ON-PEER ABUSE PLEASE REFER TO THE SAFEGUARDING POLICY.

Should a bullying incident provide you with a 'reasonable cause to suspect that a child is suffering, or likely to suffer, significant harm' this should be treated as a child protection concern and the school's safeguarding/child protection procedures should be followed.

Aims and Objectives

The ultimate aim of the Babington House School e-safety and anti-cyber bullying policy is to provide pupils, staff and parents with the tools necessary to enabling a positive relationship with technology. The policy aims to prevent bullying of any sort, ensure that everyone can use technology in a supportive, caring and safe environment without fear of being bullied.

All members of the community, including Governors, teaching and non-teaching staff, pupils and parents should have a clear understanding and respect of what bullying is and be familiar with this School policy in addition to the Anti-Bullying and Safeguarding policy.

In addition to cyber-bullying of pupils, cyber-bullying of staff, though whether by pupils, parents or colleagues, is also unacceptable.

Both E-safety and anti-cyber bullying are part of our Safeguarding provision at Babington House School.

Roles and Responsibilities	
Role	Responsibility
Designated Safeguarding Lead Elizabeth Channon	• Staff should contact any of the DSLs for advice or to report any safeguarding/child protection concerns. • To have an overview of up-to-date technology and potential technological safeguarding matters. • To arrange training for staff in e-safety. • To manage any bullying and implement procedures as set out in the anti-bullying policy. • To administer 'Safeguarding in Education' safeguarding training to staff. • To ensure cybersecurity training for staff
Deputy Designated Safeguarding Leads David Laird, Jane Hawkins, Gemma Bailey, Kate Edwards	
Health and Safety Officer Sharon Best	• To coordinate the IT Management Company
Senior IT teacher	• To provide a curriculum that promotes e-safety, pupil resilience and teaches pupils to protect themselves and their peers.

Prep IT Coordinator Maddy Pearce	To monitor the Preparatory IT curriculum that promotes e-safety, pupil resilience and teaches pupils to protect themselves and their peers.
Technical Support and IT Management Company BcTEC	- To manage IT Infrastructure and Provision for the school. - To oversee the installation and updates of SENSO (filtering and monitoring programme)
Teaching staff using screens in lessons Prep and Senior teachers	- To deliver the curriculum which incorporates regular reference and teaching of e-safety - To use SENSO in order to monitor pupils' on-screen activity - To undergo cybersecurity training - To be aware of the Government's Searching, Screening and Confiscation guidance.
Senior Leadership Team David Laird, Becky Wiffen Elizabeth Channon and Sharon Best	- To monitor the delivery of e-safety through curriculum and monitor the effective use of SENSO - To report updates and issues to the Governing Body - To regularly review the efficacy of SENSO - To undergo cybersecurity training
Governing Body Chris Turner – Chair of Governors Ben Roberts– Governor for Safeguarding Jack Magill – Governor for Education	- To ensure that e-safety and cyber bullying updates and issues are reported on and included in meetings. - To question the efficacy of SENSO in whole Governor body meetings - To attend training of cyber security

Management of IT Infrastructure and Provision

Active management of hardware, software and connectivity play a role in safety and safeguarding the school community from cyber-bullying. Our School uses BcTEC Technologies to ensure that the technical provision, infrastructure and safeguards are in place to filter and monitor inappropriate content. BcTEC also alert the school in the case of national or local safeguarding technological issues and provide advice and guidance on information that can be provided to students, parents and staff. The school uses LGFL and SENSO (security systems) to prevent/monitor access to inappropriate websites, filtering email and general use of inappropriate language etc. Email filtering to prevent SPAM and

viruses before they reach our network, Antivirus to filter data at the network gateway, email gateway, email once on the mail server and files and email once they reach our computers and servers. We also have a proxy server and firewall which is capable of scanning for inappropriate language and activity. Personal data is managed securely by BCTEC Technologies.

The DSL is the filtering and monitoring lead for the school. The Governors of the school review the effectiveness of filtering and monitoring annually. Any filtering concerns not flagged by SENSO should be flagged immediately to the DSL in person or via CPOMS.

E SAFETY AND USAGE

Our aim is to have a clear, working policy that states acceptable and unacceptable use of any internet enabled devices including but not limited to; mobile phones, computers, tablets, laptops, surfaces, chrome books, iPads/ipods, iPhones and any equipment capable of taking images as well as traditional cameras within the whole school setting, including EYFS. This policy is to be understood and adhered to by all parties concerned. Breach of this policy is deemed to be an act constituting gross misconduct.

We aim to put in place:

- Procedures for staff to follow
- Procedures for pupils to follow
- Procedures for Before and After school clubs and Holiday clubs.
- Procedures for any visitors to the school

Procedures for Staff

The use of technologies to enhance learning is encouraged. The school has a wealth of differing types of technology to provide opportunities for research, independence, investigation and develop new skills. To be able to do this effectively staff must ensure that pupils are safeguarded.

Safeguarding our children and protecting their privacy means all personal equipment belonging to staff and pupils, that are internet enabled or capable of taking images, should not be switched on in the vicinity of the children.

Staff and pupils should use the school's own IT resources for all school-based activities unless the Headmaster has approved specific exceptions. Exceptions are in place for the Sixth Form where mobile phones can be used in their Sixth Form Study Area and school provided laptops/tablets can be used as studying aids. Some pupils with SEND may also use personal devices if allowed by the SENDCO and written into an EHCP or Provision Map.

EYFS staff have access to and can use school iPads and ipods for assessment purposes. These devices must stay in school with the exception of school arranged trips. Photographs taken on these devices in the EYFS will allow pupil's achievements to be uploaded into "2 build a profile" Profile assessment system and "Evidence Me".

Caretakers, PE staff, SLT, the Marketing Manager and the School Nurse have school issued mobile phones which can be used in school, on trips and journeys.

All staff must turn off their personal mobile internet enabled devices e.g. phones and other image capable equipment during working hours and keep them secure. Such equipment should only be used during staff breaks in the designated areas (please see Acceptable use of Mobile Phone Policy) away from the vicinity of the children.

Should staff use their own mobile devices for personal use during breaks, they must do so with respect to other colleagues and whether the nature of the telephone conversation is appropriate. No member of staff should be seen during school hours with their personal mobile/internet enabled devices with the exception of the staff room, quiet working room or offices (where no children are present).

If there is a personal emergency, mobile phones may be used but such calls should be taken in a designated staff area with no pupil access.

Designated school cameras/phones can be used to take photographs of the children's learning, for assessment records, for capturing events and for the school Bulletin, as long as parents have given permission to do so. This remains in school and is only downloaded onto a school computer. Staff do not take the cameras/phones home.

Procedures for pupils

Personal mobile devices should not be in the possession of any pupil from EYFS to KS4 in the school during the school day. Emergency contact to and from parents should be made through the school office. KS5 pupils are allowed to use their mobile devices, including laptops in their study area and in lessons ONLY if their teacher has instructed them to do so.

If pupils are not in lessons, internet enabled and camera devices should only be used under supervision by a member of staff (with the exception of pupils in the Sixth Form during study periods).

Procedures for Before and After school Clubs and Holiday Club

All staff supervising Before and After-school Clubs should have personal mobile and internet enabled devices or other image capable devices, locked away while the children are present. Parents are able to contact the After-school club and Holiday Club directly from the school's main telephone system.

If a mobile phone is needed to be used in an emergency (e.g. lockdown procedure, contacting parents who use an overseas mobile number), contact should be done via one of the mobile phone supplied by the school.

Further information regarding mobile phones

Babington House ensures that all children in our care are safeguarded and their welfare is of utmost importance.

- Users bringing personal mobiles or other data holding devices into Babington House must ensure that there are no inappropriate images or illegal content on the device.

- Staff should ensure that the office has up to date contact information and that staff will make their families, children's schools aware of work telephone numbers in the case of emergency. With the benefit of telephones in all teaching areas it is possible for calls to be quickly forwarded onto individual staff.
- Mobile phones, iPods, iPads or other communication devices are prohibited in all areas of Babington House School with the exception of the staff rooms and staff offices when pupils are not present.
- During trips, school mobile phones will be allocated to teachers.

Exceptions

If individual members of staff should need, for a specific reason, to have their mobile phone with them outside the policy procedures, they must gain permission from the Head of Preparatory Mr James Mole, the Head of Seniors Mr Paul Showell, the Deputy Head of Preparatory, Miss Kate Edwards or the Headmaster Mr Tim Lello.

ANTI CYBER BULLYING

Definition

Childline defines cyber-bullying as "using the internet, email, online games or any digital technology to threaten, tease, upset or humiliate someone else." The school considers online safety as part of both safeguarding and anti-bullying arrangements. Examples include using social networking websites, mobile phones, text messaging, photographs, video, e-mail, sexting, online gaming, abusing personal information, instant messaging and chat rooms and online grooming.

Child on Child abuse can occur through cyber-bullying and will be managed through the anti-bullying systems (please see anti-bullying policy). If the cyber-bullying incident demonstrates a 'reasonable cause to suspect that a child is suffering, or likely to suffer, significant harm' this should be treated as a child protection concern and the school's safeguarding/child protection procedures should be followed.

There are 4 areas of online risk and we recognise that these are:

Four areas of online risk explicitly defined:

- Content
- Contact
- Conduct
- Commerce

We recognise that significant harm to students can be through:

- - Cyber-flashing
 - Online exploitation
 - Radicalisation pathways
 - Mis/disinformation
 - AI misuse

Reporting Mechanisms for Cyber Bullying

- Pupils should report any issues related to cyber-bullying to a member of staff they feel comfortable with.
- All pupils are frequently informed of the school's DSLs through planners, form times, assemblies and permanent display boards.
- All staff should follow the processes stated in the Anti-Bullying Policy and Behaviour and Discipline Policy.
- If the report is of a child protection nature, the Safeguarding reporting process should be followed using CPOMS and DSLs informed immediately.

Sanctions for cyber-bullying

Harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations, webcam photography or face-to-face meetings. The school's Anti-Bullying policy and Safeguarding Policy explains further how we try to keep pupils safe in school. Cyber-bullying by pupils will be treated as seriously as any other type of bullying and will be managed through our anti-bullying procedures

- Cyber-bullying will be treated following the same process as listed in the anti-bullying policy and in the Behaviour and Discipline Policy.
- If the Cyber-bullying is of an illegal nature, the DSLs will be informed who will contact and report to the Police and MASH team.
- If the Cyber-bullying is of a child protection /safeguarding concern the DSLs will be informed through CPOMS and verbally and this will be dealt with through the Safeguarding children procedures.

The School reserves the right to review electronic material held or accessed by any pupil in school including their school email account and their mobile phone.

Where any form of cyber bullying affects another pupil in the School or may bring the reputation of the School into disrepute, the School reserves the right to be involved whether the incident(s) took place within the School or externally.

Keeping Pupils informed and building resilience.

Pupils will often have access to technologies that have both positive and negative potential. Most of our pupils will use internet enabled devices including mobile phones and computers/tablets/laptops at home on their own devices or in school on school devices.

The school teaches pupils techniques, strategies and skills to enable them to protect themselves and their peers. Pupils are educated in how to protect themselves online both at home and at school, they are provided with current information to guide them to make sensible choices and to know what to do if they are subjected to cyber bullying or issues of a child protection nature.

Both E-Safety and Anti-Cyber Bullying are included within the curriculum and wider school activities including but not exclusively; workshops, assemblies, PSHE, ICT and Form Time.

They are also given clear and thorough training of the dangers of online abuse and how to avoid them and to build independent resilience. This is delivered within the context of the benefits of the internet to build resilience and self-protective lifelong skills. These are delivered by school staff and external specialists.

Pupils are made aware that some forms and levels of cyber bullying are illegal and the School will inform the police when necessary.

Staff Training

Staff are trained in online safety through the 'Safeguarding In Education' online course, through external providers and through updates from the IT teachers, Designated Safeguarding Leads (and Deputies) and BCTEC Technologies.

Staff are encouraged to discuss e-safety and anti-cyber bullying safeguarding strategies with pupils in a cross curricular way e.g. During form time, within a lesson that is incorporating technology, PSHE discussions and assemblies.

Parental updates

Parents are provided with information and advice regarding online safety with their children at home. Parents are sent communications by the Designated Safeguarding Leads if there are any current local or national issues that parents need to be made aware of. Parents are also invited to attend Online Safety workshops run by an external specialist.

Management of Personal Data

Please see Data Protection Policy.