ABBEY COLLEGE IN MALVERN
abbeycollege.co.uk

Online Safety Policy

Related documents include:
• KCSIE 2023 • Introduction to the Academic courses offered at the Abbey College • Examinations Policy and previous examination papers • Academic Staff Handbook • Student Handbook • Induction for students • Individual Course Overviews • Schemes of Work • RSHE curriculum • Prevent Duty • Keeping children safe in Education • Sharing nudes and semi-nudes • Cyberbullying • Sexual Violence & harassment between children in schools & colleges
Legal Status:
• Malicious Communication Act 1988 • Children Act 1989 • Computer Misuse Act 1990 • Communications Act 2003 • The Prevent Duty Guidance 2015 • Digital Economy Act 2017 • Age-Appropriate design code 2020 • GDPR Act 2018 • Young People & Gambling 2019
Monitoring and Review
• This policy will be subject to continuous monitoring, refinement and audit by the Principal. • The Principal will undertake a formal annual review of this policy for the purpose of monitoring and of the efficiency with which the related duties have been discharged, by no later than one year from the date shown below, or earlier if significant changes to the systems and arrangements take place, or if legislation, regulatory requirements or best practice guidelines so require.
• The next official date for review is **October 2024**

Online Policy

Information and Communication Technology (ICT) has transformed the process of teaching and learning in the College. It is a crucial component of every academic subject, and is also taught as a subject in its own right. The majority of our students are taught how to research on the internet and to evaluate sources. They are instructed in the importance of evaluating the intellectual integrity of different sites, and why some apparently authoritative sites need to be treated with caution.

ICT and the communications revolution provide unrivalled opportunities for enhanced learning, but also pose risks to young people. We therefore teach students how to stay safe in this environment and how to mitigate risk, including identity theft, bullying, harassment, grooming, stalking, radicalisation and abuse. They also need to learn how to avoid the risk of exposing themselves to subsequent embarrassment.
This policy should be read in conjunction with the following policies: Child Protection, Procedures for Responding to Concerns About a Child or Young Person's Wellbeing, Dealing with Allegations of Abuse Made Against a Child or Young Person, Managing Allegations Against Staff and Volunteers, Code of Conduct for Staff and Volunteers, Anti-Bullying Policy and Procedures, Photography and Image Sharing Guidance.

Child Protection

As a College we recognise that internet safety is a child protection and general safeguarding issue. All staff at the College attend Online training at least once annually. Updates to training are carried out termly by DSL at the college. All Staff must complete online Educare Course to keep their knowledge current and up to date. They work to promote a culture of responsible use of technology that is consistent with the ethos of the College. All of the staff, especially those with boarding responsibilities, receive annual in-house training in online safety issues.

We have a programme on online safety (incorporated into the Citizenship syllabus) which ensures that all year groups in the College are educated, in an age-appropriate way, in the risks and reasons why they need to behave responsibly online. The Principal is responsible for overseeing the programme.

As a College, we will not tolerate any illegal material. If we discover that a child or young person is at risk as a consequence of online activity, we may seek assistance from the Child Exploitation and Online Protection Unit (CEOP). We will impose a range of sanctions on any student who misuses technology to bully, harass or abuse another student in line with our Anti-bullying Policy.

Online Safety is a whole college responsibility, and all staff and students are required to adhere to an ICT Acceptable Use Policy which incorporates the following guidelines in age appropriate ways:

- We expect students to treat staff and each other online with the same standards of consideration and good manners as they would in the course of face-to-face contact.
- We expect a degree of formality in communications between staff and students, and would not in normal circumstances expect them to communicate with each other by text or mobile phone.
- Everyone has a right to feel secure and to be treated with respect, particularly the vulnerable. Harassment and bullying will not be tolerated. The College is strongly committed to promoting equal opportunities for all, regardless of race, gender, religious affiliation, cultural background, gender orientation or disability.

If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.

Cyberbullying

- Cyberbullying is a particularly pernicious form of bullying, because it can be pervasive and anonymous. There can be no safe haven for the victim, who can be targeted at any time or place. The College's Anti-Bullying Policy sets out our preventative measures and the procedures that will be followed where we discover cases of bullying.
- Proper supervision of students plays an important part in creating a safe ICT environment at school, but everyone needs to learn how to stay safe when using the internet unsupervised
- Bullying and harassment in any form should always be reported to a member of staff. It is never the victim's fault, and he or she should not be afraid to report the matter.

Keeping the College's Network Safe

Certain sites are blocked by the College's filtering system and the system monitors all use of the network and the Network Manager will check this on a regular basis, under the direction of the Bursar.

- The system also monitors e-mail traffic and blocks SPAM and certain attachments.
- There is strong anti-virus protection on our network, which has been installed by the IT Support.
- Any member of staff or student who wishes to connect a laptop or handheld device to the College's network must do so using the Wi-Fi system which is subject to the College filtering and logging systems.

Acceptable Use Policies for ICT usage are given to all staff and students. The College will impose sanctions for the misuse, or attempted misuse of the internet, mobile phones and other electronic devises.

The **College Network Manager** has a key role in maintaining a safe technical infrastructure at the College and in keeping abreast with the rapid succession of technical developments. They are responsible for the security of our system and data. They monitor the use of the internet and e-mails and will report any observed inappropriate usage to the appropriate senior manager. It is the responsibility of all staff to report any inappropriate usage to the Bursar.
Access to sites of inappropriate content is blocked from the College network, as is access to social networking sites such as Facebook on school room computers. Boarders have access to Facebook in the evenings, but this is monitored by staff in the boarding houses on a regular basis through discussions with the students.

Social Networking Sites and Telephone Communication

In normal circumstances, staff should **not** share personal contact details with students and this includes mobile telephone numbers, (with the exception of members of the boarding team & staff on excursions duty), home telephone numbers, instant messaging identities and social network screen-names. Where this is deemed to be needed for any reason, staff should first discuss the matter with the welfare manager or the Principal. Staff and students should not have each other as contacts on their personal social networking sites. Staff should not request, or respond to, any personal information from the child/young person other than that which might be appropriate as part of their professional role. If queries exist or if advice is needed, staff should consult the Principal.

Personal e-mail addresses, instant messaging identities or personal telephones (mobile or fixed line) should never be used to contact students without the explicit agreement of the Principal.

Students should not take images (for example, video or photographs) of staff or students **without their permission** and any images should only be shared with the express permission of those involved.

Particular issues may arise as a consequence of the ability to create, to store and to manipulate video and photographic images. The safest approach is to avoid using personal equipment and to use a work-provided item for this task. This may not always be possible and the requirements outlined here are aimed at guiding staff and students to safe outcomes.

Video and Photographic Images

Staff need to be mindful of the possible child protection issues associated with the possession of images of children and as such they are required to adhere to the following policy.

- All images and video taken of individual students or groups of students must be uploaded **as soon as possible** to the College network and then **deleted** immediately from any personal computer, the hard drive of any computer, the memory of any camera or similar device, any personal memory device or other transportable memory.
- All images and video of individual students or groups of students which are delivered to a member of staff as part of their professional work, for example, for an Art display or a marketing initiative, must **not** be stored on any personal computer, the hard drive of any school computer, the memory of any camera or similar device, any personal memory device or other transportable memory and should be uploaded immediately to the College network.
- Any manipulation or images or video for any purpose including controlled assessment, coursework, marketing, etc, **must** be undertaken on the College network and the results of that manipulation stored on the network only. Exceptionally, Heads of Department may have occasion to transmit appropriate video and images to the awarding bodies and will be guided in that by the relevant regulations.

ICT has transformed the ways we communicate with others, both in and out of the classroom. Our aim is to promote the positive use of this technology and to discourage inappropriate usage or usage which could put others at risk. Staff are asked to recognise that this policy is designed above all to protect the interests of the child, to support staff and to ensure that required action is taken as quickly as possible.

Staff Training repeated above

Staff receive mandatory annual training in child protection and online safety. They are also asked to complete the Educare module 'Child Exploitation and Online Safety for Education'.

How Will Student Infringements be Handled?

Whenever a student infringes the Online Safety Policy, the final decision on the level of sanction will be at the discretion of the College management.

The following are set out as guidance based on the level of infringement:

Category A Infringements

- Use of non-educational sites during lessons
- Unauthorised use of e-mail
- Unauthorised use of mobile phone (or other new technologies) in lessons; for example, to send texts to friends
- Use of unauthorised instant messaging/social networking sites

Possible sanctions: referred to class teacher for a warning and clarification of what can happen if this is repeated, mobile phone removed from student and passed to either the Principal for collection at the end of the school day.

Category B Infringements

- Continued use of non-educational sites during lessons after being warned
- Continued unauthorised use of e-mail after being warned
- Continued unauthorised use of mobile phone (or other new technologies) in lessons after being warned
- Continued use of unauthorised instant messaging/chat rooms/social networking sites
- Use of file sharing software for the purposes of sharing music, games or videos illegally
- Accidentally corrupting or destroying others' data without notifying a member of staff of it
- Accidentally accessing offensive material and not logging off or notifying a member of staff of it

Possible sanctions: referred to class teacher or Head of Department for follow-up action which could include detention or removal of internet and/or e-mail access for a period of time / mobile phone removed from student and passed to a Senior member of staff.

Category C Infringements

- Deliberately corrupting or destroying someone's data, violating the privacy of others
- Sending a **one-off** e-mail or text message that is regarded as harassment or of a bullying nature
- Deliberately trying to access offensive, radicalisation or pornographic material including sexting
- Transmission of commercial or advertising material

Possible sanctions: referred to Principal for a warning and clarification of what can happen if this is repeated and contact with parents. If inappropriate web material is accessed, then ensure the Network Manager is informed and that appropriate technical support filters the site.

Category D Infringements

- Continued sending of e-mails or text messages regarded as harassment or of a bullying nature after being warned
- Uploading any information of other people to social networking sites without permission including and not limited to comments, drawings, photographs, videos
- Deliberately accessing, downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic, related to radicalisation or violent
- Receipt or transmission of material that infringes the copyright of another person or infringes the conditions of the Data Protection Act, revised 1998
- Bringing the school name into disrepute
- Using the school network as a means of inciting riot or public order offences

Possible sanctions: referred to the Principal, who will contact their parents and may include exclusion as well as referral to the Community Police / removal of technological device. If appropriate, secure and preserve any evidence; for example, print-outs of e-mails/texts and inform the sender's service provider.

What do we do if...

...an inappropriate website is accessed unintentionally in school by a teacher or child?

1. Play the situation down; don't make it into a drama.
2. Report to the Principal who will inform IT Support and ensure the site is filtered.

...an inappropriate website is accessed intentionally by a child?
1. Refer to the guideline sanctions referred to in this policy
2. Notify the parents of the child of the sanctions imposed and of any other concerns arising.
3. Notify the Principal, who will inform IT Support and ensure the site is filtered.

...a bullying incident directed at a child occurs through e-mail, social media or mobile phone technology?
1. Advise the child not to respond to the message.
2. Refer to the Anti-Bullying Policy and apply appropriate sanctions.
3. Secure and preserve evidence where possible.
4. Immediately inform the Principal.
5. The Principal will address the issue with the relevant students and consider opportunities to address the issues raised in a wider context, e.g. assemblies, citizenship session, house meetings, etc.

…inappropriate photographs, videos are sent to a student via mobile phone or social networking sites.
1. Advise the child not to respond to the message.
2. Refer to the Anti-Bullying Policy and apply appropriate sanctions.
3. Secure and preserve evidence where possible.
4. Immediately inform the Principal
5. The Principal will address the issue with the relevant students and consider opportunities to address the issues raised in a wider context, e.g. Assemblies, Citizenship session, House Meetings, etc.

...malicious or threatening comments are posted on an Internet site about a student or member of staff.
1. Inform and request the comments be removed if the site is administered externally.
2. Secure and preserve any evidence.
3. Send all evidence to CEOP at **www.ceop.gov.uk/contact_us.html**
4. Endeavour to trace the origin and inform the police as appropriate.

...you are concerned that a child's safety is at risk because you suspect someone is using communication technologies (such as social networking sites) to make inappropriate contact with the child.
1. Report to and discuss with the College DSMS (Principal, or in his absence, Steph Chadderton, Matron)
2. Advise the child on how to terminate the communication and save all evidence.
3. Contact CEOP http://www.ceop.gov.uk/
4. Consider the involvement of police and children's social care.

All incidences involving online safety should be reported to the Principal