ABBEY COLLEGE IN MALVERN
abbeycollege.co.uk

Online Safety Policy

Related documents include:

- 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 2026
- Sharing nudes and semi-nudes: advice for education settings
- Cyberbullying
- Sexual Violence & harassment between children in schools & colleges
- Child Protection and Safeguarding Policy
- 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
- ICT Acceptable Use Policies for staff and students
- Data Protection / Privacy Notice and records-management arrangements

Legal Status and Statutory/Regulatory Framework:

This policy should be read and applied in accordance with the legislation and statutory guidance relevant to the College. The principal references include:

- Children Act 1989 and Children Act 2004.
- Education Act 2002, including the safeguarding duties relevant to independent schools, and the Education (Independent School Standards) Regulations 2014 (as amended), particularly the requirements concerning safeguarding and welfare.
- Keeping Children Safe in Education 2026 (KCSIE), statutory guidance for schools and colleges, in force from 1 September 2026.
- Counter-Terrorism and Security Act 2015, section 26, and the Prevent duty guidance applicable in England.
- Equality Act 2010.
- UK General Data Protection Regulation (UK GDPR), the Data Protection Act 2018, as amended, and the Data (Use and Access) Act 2025, together with applicable privacy and electronic communications requirements.
- Online Safety Act 2023, including the framework regulating relevant user-to-user and search services and the communications offences provided for by the Act.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

- Computer Misuse Act 1990.
- Communications Act 2003 and the Malicious Communications Act 1988, as amended and subject to the communications-offence changes made by the Online Safety Act 2023.
- Protection of Children Act 1978 and Criminal Justice Act 1988, section 160, in relation to indecent images of children.
- Sexual Offences Act 2003, including offences relevant to grooming and sexual communication with a child.
- Voyeurism (Offences) Act 2019 and relevant provisions concerning the taking or sharing of intimate images.
- Copyright, Designs and Patents Act 1988.
- Digital Economy Act 2017, where relevant.
- Age Appropriate Design Code (Children's Code), issued by the Information Commissioner under the Data Protection Act 2018.
- Department for Education filtering and monitoring standards and relevant digital and technology standards for schools and colleges.

The list is not exhaustive. The College will have regard to relevant statutory guidance and official advice as it is updated. The Online Safety Act 2023 places duties principally on providers of regulated online services; this policy does not suggest that every provider duty applies directly to the College. The Act is relevant to the online environment, harmful content and communications offences that may affect students and staff.

The Data (Use and Access) Act 2025 amends, rather than replaces, the UK GDPR and Data Protection Act 2018. The College will apply the data protection framework as amended and will keep its privacy and information-handling arrangements under review.

Monitoring and Review

- This policy will be subject to continuous monitoring, refinement and audit by the Welfare Manager.
- The Welfare Manager 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 College will also review its filtering and monitoring provision at least annually and following any significant change in technology, online risks, systems or safeguarding arrangements. The review will involve the DSL, senior leadership and IT support, with appropriate assurance provided to the Proprietor.

- The next official date for review is **October 2027**.

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.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

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.

Online safety includes the safe and responsible use of internet-connected devices, social media, messaging services, gaming platforms, video-sharing platforms, email, cloud services, generative artificial intelligence (AI), image and video manipulation tools and other digital technologies. Risks may include contact, conduct, content and commerce risks, as well as misinformation, scams, exploitation, extremism, harmful challenges, self-harm content and inappropriate or discriminatory material.

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 the DSL at the College. All staff must complete the required 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.

Staff training will reflect the current version of Keeping Children Safe in Education and the College's safeguarding procedures. Staff must understand how to recognise and report online safeguarding concerns, including concerns arising from peer-on-peer abuse, sexual harassment, sexual violence, coercion, exploitation, grooming, radicalisation, cyberbullying, self-harm and suicide-related content, and the creation or circulation of manipulated or AI-generated images.

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. Online safety education will be reviewed regularly and will address safe searching, privacy, digital footprints, respectful communication, misinformation, online relationships, reporting harmful content, image sharing, scams, gaming and AI.

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 (CEOP) Safety Centre, the police or children's social care, as appropriate. 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.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

Online safety is a whole College responsibility. 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.

Students must not use digital technology to threaten, intimidate, humiliate, impersonate, exploit or discriminate against another person. They must not create, request, possess, store or share sexualised or intimate images of themselves or others. Any concern involving a student and an intimate image must be referred immediately to the DSL or DDSL and managed in accordance with current government guidance. Staff must not ask a student to forward, download or show an indecent image, or copy, print, save or distribute it.
Where AI or image-editing tools are used to create or alter an image, audio recording or video of a student or member of staff, this will be treated seriously, including where the material is fabricated, sexualised, humiliating or shared without consent. The absence of an authentic photograph or recording does not make such conduct harmless.

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.

All concerns must be reported promptly to the DSL or DDSL. Staff must not investigate allegations themselves, promise confidentiality, or delay reporting while attempting to establish whether the concern is substantiated. The College will follow its safeguarding procedures, including referral to external agencies where required.

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.

Cyberbullying includes abuse through social media, messaging, email, gaming, group chats, image or video sharing, impersonation, exclusion, threats, doxxing and the repeated sharing of humiliating or manipulated content. It may take place outside College hours or away from the College site but will be addressed where it affects the safety, welfare or education of students or the College community.

Keeping the College's Network Safe

Certain sites are blocked by the College's filtering system and the system monitors use of the network. 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 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 devices.

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 and any safeguarding concern to the DSL or DDSL.

Access to sites of inappropriate content is blocked from the College network, as is access to social networking sites such as Facebook on schoolroom 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.

Filtering and monitoring are complementary safeguards: filtering seeks to prevent access to illegal, inappropriate or harmful content, while monitoring identifies and supports a response to concerning activity. The College will ensure that filtering and monitoring are proportionate, effective and appropriate to the age and needs of students, including the risks presented by AI-generated content, applications and services.

The Proprietor and senior leadership will ensure that responsibility for filtering and monitoring is allocated clearly. The DSL will lead on safeguarding decisions and review relevant alerts and reports with IT support. IT support will maintain the technical systems, provide reports and take agreed

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

technical action. Senior leadership will oversee the system, record decisions about what is blocked or permitted, and ensure that staff understand how to report concerns.

The College will review filtering and monitoring at least annually, test that systems are working as intended, consider whether mobile and personal devices using College networks are covered, and act promptly on identified weaknesses. Monitoring will be carried out lawfully, transparently and proportionately, with regard to data protection and staff/student privacy. Users will be informed through the relevant Acceptable Use Policies that College systems may be monitored.

The College will maintain appropriate cyber security measures, including access controls, secure configuration, anti-malware protection, updates, backups and procedures for responding to suspected cyber incidents. Suspected compromise, phishing, malware, unauthorised access, data loss or disclosure must be reported promptly to IT support and the Bursar; any safeguarding implications must also be reported to the DSL.

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 and 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.

Staff must use College-approved accounts, platforms and communication channels for professional contact with students wherever available. Any permitted exception must be authorised in advance by the Principal and must be transparent, recorded where appropriate and consistent with the staff Code of Conduct. Staff must not communicate with students through disappearing-message services or private social media accounts.

Students should be encouraged to use privacy settings, strong and unique passwords, multi-factor authentication where available, and to avoid sharing personal information, location data, passwords or security codes. Students should be aware that online posts, images and messages may be copied, retained or redistributed even after deletion.

Video and Photographic Images

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

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

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.

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 of 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.

The College will obtain and record appropriate permissions for the use of student images, explain the purposes for which images may be used, and handle images in accordance with its data protection obligations and relevant privacy notices. Images must only be accessed by staff who need them for an authorised purpose and must be retained and deleted in accordance with College retention arrangements.
Images, video or audio must not be altered or used to ridicule, sexualise, impersonate, threaten or otherwise harm a student or member of staff. The creation or circulation of fake or AI-generated intimate images, including so-called deepfakes, is prohibited and will be treated as a serious safeguarding matter.

Where an image may be an indecent image of a child, staff must not copy, download, print, forward or otherwise distribute it. Do not ask a student to send or forward it. Preserve relevant contextual information safely (for example, the platform, account name, URL, date and time) without circulating the image, and immediately refer the matter to the DSL or DDSL. The DSL will determine the appropriate safeguarding and external referral response in accordance with current guidance and police advice.

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

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

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'.

Training will be refreshed when there are significant changes in legislation, statutory guidance, College systems or the nature of online threats. Staff must know how to report a safeguarding concern, a technical incident and a data protection incident, and understand that these may require separate but coordinated reporting.

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:

- 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.
- 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.
- 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 data protection legislation.
- Bringing the College name into disrepute.
- Using the College network as a means of inciting riot or public order offences.
- Creating, requesting, sharing or threatening to share intimate images, including manipulated or AI-generated sexual images; impersonating another person; or using technology to exploit, groom, threaten or coerce another person.
- Attempting to bypass College filtering, monitoring or cyber security controls, or accessing another person's account or data without authority.

Possible sanctions at lower levels: referred to the DSL or 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.

Possible sanctions at a higher level: referred to the DSL or Principal, who will contact parents and may include exclusion as well as referral to the police or other relevant agencies / removal of a technological device where lawful and appropriate. If appropriate, secure and preserve evidence in accordance with safeguarding and data protection procedures. Staff must not circulate potentially illegal images or conduct their own investigation.

Sanctions will be proportionate, take account of the age and understanding of the student and any relevant additional needs, and will not replace safeguarding action or referral where a child may be at risk. The College will consider the welfare and support needs of any student affected, including bystanders.

What do we do if...

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

...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 Director, who will inform IT Support and ensure the site is filtered as appropriate. If the material raises a safeguarding concern, inform the DSL or DDSL immediately.

...an inappropriate website is accessed intentionally by a child?

3. Refer to the guideline sanctions referred to in the College Rules and Justice System Booklet.
4. Notify the parents of the child of the sanctions imposed and of any other concerns arising, where appropriate and consistent with safeguarding advice.
5. Notify the Director, who will inform IT Support and ensure the site is filtered as appropriate.
6. Refer any safeguarding concern to the DSL or DDSL, who will consider whether external advice or referral is required.

...a bullying incident directed at a child occurs through e-mail, social media or mobile phone technology?

7. Advise the child not to respond to the message.
8. Refer to the Anti-Bullying Policy and apply appropriate sanctions.
9. Secure and preserve evidence where possible, without forwarding or redistributing harmful or potentially illegal images.
10. Immediately inform the Principal or Welfare Manager and the DSL or DDSL.
11. The Principal, Welfare Manager or DSL 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 or videos are sent to a student via mobile phone or social networking sites?

12. Advise the child not to respond to the message or forward it.
13. Refer to the Anti-Bullying Policy and apply appropriate sanctions where relevant.
14. Do not ask the student to forward, download or show an indecent image. Do not copy, print or distribute the image.
15. Immediately inform the Principal or the Welfare Manager and the DSL or DDSL.
16. The DSL will follow current safeguarding guidance, consider the welfare of all students involved and make referrals to the police or other agencies where appropriate.

...malicious or threatening comments are posted on an Internet site about a student or member of staff?

17. Inform the relevant senior member of staff and, where appropriate, request removal of the comments if the site is administered externally.
18. Secure and preserve relevant evidence, such as the URL, account details, date/time and screenshots of non-indecent content, where lawful and safe to do so.
19. Refer safeguarding concerns to the DSL or DDSL. The DSL will consider whether to contact CEOP, the police, the platform or other relevant agencies.
20. Endeavour to identify the source only where appropriate and lawful; staff must not undertake intrusive or unsafe investigations.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026

...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?

21. Report to and discuss with the College DSL or DDSL immediately.
22. Listen to the child, reassure them and do not promise confidentiality. Do not confront the suspected perpetrator or investigate independently.
23. Preserve relevant evidence safely and do not delete messages or accounts before advice has been obtained. Do not copy or distribute indecent images.
24. The DSL will consider the appropriate response, including CEOP, the police and children's social care, as appropriate.

...a member of staff becomes aware of a data breach, cyber incident or unauthorised access to personal information?

25. Report it immediately to the Bursar / relevant senior manager and IT support, and to the DSL where there may be a safeguarding impact.
26. Do not attempt to conceal, delete or independently investigate the incident. Preserve relevant information and follow the College's data breach and cyber incident procedures.
27. The College will assess the incident, take steps to contain it and consider whether notification to the Information Commissioner's Office or affected individuals is legally required.

All incidences involving online safety should be reported to the DSL or DDSL. Technical or data security incidents must also be reported through the College's IT and data protection procedures.

Abbey College in Malvern Ltd (Number 08661073)
Registered in England and Wales. Registered office: 253 Wells Road, Malvern, Worcestershire, WR14 4JF
Member of ENGLISH UK, Accredited by the British Council for the teaching of English in the UK, DfES Reg. No. 8856026