



S69 ONLINE SAFETY POLICY

Reviewed: Education and Policy Committee
Approved: Full Governing Body

Approved Date: November 2025
Next Review Date: November 2026

CONTENTS

1.	INTRODUCTION.....	4
2.	MAKING USE OF IT AND THE INTERNET IN THE CHOIR SCHOOL	5
3.	IMPORTANCE	5
4.	RESPONSIBILITIES	6
5.	EDUCATION AND TRAINING	9
6.	CYBERBULLYING	10
7.	THE THREAT OF ONLINE RADICALISATION	11
8.	RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS.....	11
9.	MONITORING AND FILTERING	12
10.	ONLINE SAFETY REVIEW	14
11.	SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS	15
12.	EMAILS.....	15
13.	SAFE USE OF DIGITAL AND VIDEO IMAGES OF PUPILS.....	16
14.	SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING.....	19
15.	USE OF SCHOOL AND PERSONAL MOBILE PHONES AND DEVICES	20
16.	LIVE STREAMING & TELEVISION BROADCASTS	24
17.	MANAGEMENT OF APPLICATIONS WHICH RECORD CHILDREN'S PROGRESS (DATA AND IMAGES)	24
18.	MANAGING EMERGING TECHNOLOGIES.....	24
19.	PROTECTING PERSONAL DATA.....	25
20.	BREACHES OF POLICY BY EMPLOYEES	25
21.	VISITORS' USE OF MOBILE AND SMART TECHNOLOGY.....	25
22.	COMPLAINTS	26
	APPENDIX 1: INTERNET ACCESS AND ELECTRONIC SAFETY IN BOARDING.....	27
	APPENDIX 2: SOURCES OF INFORMATION FOR SCHOOLS AND PARENTS TO KEEP CHILDREN SAFE ONLINE	28

1. INTRODUCTION

Westminster Abbey Choir School recognizes that IT and the internet are fantastic tools for learning and communication that can be used in school to enhance the curriculum, challenge pupils, and support creativity and independence. Using IT to interact socially and share ideas can benefit everyone in the school community, but it is important that the use of the Internet and IT is seen as a responsibility and that pupils, staff and parents use it appropriately and maintain good practice online. It is important that all members of the Foundation community are aware of the dangers of using the internet and how they should conduct themselves online.

Online safety covers the Internet, but it also covers mobile phones and other electronic communication technologies. We know that some adults and young people may attempt to use these technologies to harm children. The harm might range from sending hurtful or abusive texts and emails, to enticing children to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

There is a 'duty of care' for any persons working with children. Educating all members of the school community on the risks and responsibilities of online safety falls under this duty. It is important that there is a balance between controlling access to the Internet and technology and allowing freedom to explore and use these tools to their full potential. This policy aims to be an aid in regulating IT activity in the school and provide a good understanding of appropriate IT use that members of the school community can use as a reference for their conduct online both inside and outside of school hours.

Online safety is a whole-school issue and responsibility.

The school is conscious of its additional responsibilities to monitor the use of Digital Technology by its boarding pupils. The Designated Safeguarding Lead has overall responsibility for the online safety of pupils who board. Boarding Pupils are obliged to comply with the provisions of the Boarding Handbook which contains specific guidance on Online Safety. The relevant section is annexed to this Policy in Appendix 1.

This policy and our requirements for the Acceptable Use of IT within the school cover both fixed and mobile internet devices provided by the school (such as PCs, laptops, webcams, tablets, whiteboards, digital video equipment, etc.); as well as all devices owned by pupils and staff brought onto school/school premises (personal laptops, tablets, wearable technology e.g. smart phones and watches, etc.). They also cover when pupils are going online in the home environment, for example when accessing remote learning.

This policy should be read in conjunction with the following policies/guidance for further clarity:

- S11: Safeguarding Policy
- S23: Anti-Bullying Policy
- S03: Behaviour, Discipline and Exclusions Policy
- S57: Staff Code of Conduct
- S65: Boarding Handbook for Pupils
- S13: Relationships and Sex Education (PSHE and RSE) Policies

- S43: School Trips and Educational Visits Policy
- S06: Data Protection Policy & Privacy Notice
- S48: Use and Storage of Images of Children Policy
- S07: Equality, Diversity and Inclusion Policy
- S52: Whistleblowing Policy
- DfE Guidance on Teaching Online Safety in Schools (June 2019, updated Jan 2023) [Teaching online safety in schools - GOV.UK](#)
- Keeping Children Safe in Education 2025 (KCSIE) [Keeping children safe in education - GOV.UK](#)
- UKCIS Education for a Connected World Framework [Education for a Connected World - GOV.UK](#) (June 2020)

The school will operate its policy in accordance with Westminster City Council's inter-agency procedures. See London Child Protection Procedures (updated 26th September 2025) a copy of which is available from: <https://www.londoncp.co.uk/>

2. MAKING USE OF IT AND THE INTERNET IN THE CHOIR SCHOOL

The Internet is used in the Choir School to raise educational standards, to promote pupil achievement, to support the professional work of staff and to enhance the school's management functions. Technology is advancing rapidly and is now a huge part of everyday life, education and business. We want to equip our pupils with all the necessary IT skills that they will need to enable them to progress confidently into a professional working environment when they leave school. However, we also need to prepare the pupils for the more subtle risks that go hand in hand with technology. Our pupils are therefore not just taught to use the internet and information communication technology, but how to stay safe in the online environment and how to mitigate risks.

3. IMPORTANCE

The school acknowledges the provisions of KCSIE (2025) which states: 'Technology is a significant component in many safeguarding and wellbeing issues'. Children are at risk of abuse online as well as face to face. In many cases abuse will take place concurrently via online channels and in daily life. Technology can often provide a platform which facilitates child sexual exploitation, radicalisation, and sexual predation. An effective approach to online safety therefore empowers a school to protect and educate the whole school community in their use of technology and establishes mechanisms to identify, intervene in, and escalate any incident where appropriate.

The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content. For example, pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, extremism, misinformation, disinformation and conspiracy theories
- **Contact:** being subjected to harmful online interaction with other users. For example, peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes.

- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm. For example, making, sending and receiving explicit images (including consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying.
- **Commerce:** being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams.

4. RESPONSIBILITIES

Online Safety Lead and DSL
The Abbey Head of ICT

Chloe McNeely
Stuart Winter

The designated member of the governing body responsible for online safety is Robert Gullifer, Governor with responsibility for Safeguarding.

4.1 Governors

In line with KCSIE (2025), the Board of Governors holds online safety as a central theme in their whole-setting approach to safeguarding. It is essential that pupils are safeguarded from potentially harmful and inappropriate online material. Their approach to online safety empowers the school to protect and educate pupils and staff in their use of technology, with mechanisms in place to identify, intervene in, and escalate any concerns where appropriate.

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy by reviewing online incidents and monitoring reports. Online safety falls within the remit of the Governor responsible for Safeguarding.

The role of the Online Safety Governor will include:

- ensuring an online safety policy is in place, reviewed every year and/or in response to an incident and is available to all stakeholders
- ensuring that the school has a DSL with responsibility for online safety who has been trained to a level of knowledge which is relevant to the school, up to date and progressive
- ensuring that safeguarding training for staff, including online safety training, is integrated and considered as part of the whole school safeguarding approach
- ensuring that pupils are taught about safeguarding, including online safety
- ensuring that procedures for the safe use of IT and the Internet, including appropriate online filtering and monitoring systems, are in place and adhered to holding the Headteacher and staff accountable for online safety

4.2 Headteacher and Senior Leadership Team

The Headteacher has a duty of care for ensuring the safety (including online safety) of members of the school community, though the day-to-day responsibility for online safety will be delegated to the DSL, who is the appointed Online Safety Lead. Any complaint about staff misuse of technology in the school must be referred to the Headteacher as a safeguarding issue

involving a member of staff, or for wider Abbey staff to Dave Pate, Abbey Safeguarding Officer.

The role of the Headteacher will include:

- i. Ensuring access to induction and training in online safety practices for all users
- ii. Ensuring all staff receive regular, up to date training
- iii. Ensuring appropriate action is taken in all cases of misuse
- iv. Working with the Abbey's IT Manager to ensure that Internet filtering methods are appropriate, effective and reasonable
- v. Ensuring that pupil or staff personal data, as recorded within school management system, sent over the Internet is secured
- vi. Working in partnership with the Department for Education (DfE) and the Abbey IT Manager to ensure systems to protect pupils are appropriate and managed correctly
- vii. Working with the Abbey IT Manager to ensure the IT system is reviewed regularly regarding security and that virus protection is installed and updated regularly

4.3 Designated Safeguarding Lead

The DSL is acknowledged as having overall responsibility for online safeguarding within school, including online filtering and monitoring. The DSL and leadership teams follow the guidance regarding online safety within 'Keeping Children Safe in Education' 2025; and the DfE guidance outlining how schools can ensure their pupils understand how to stay safe and behave online as part of existing curriculum requirements.

Their role includes:

- i. Being able to understand the unique risks associated with online safety, including the additional risks faced by pupils with SEND
- ii. Leading safeguarding, including online safety, meetings
- iii. Liaising with staff (especially pastoral support staff, school Matron, IT and SENDCO) on matters of safety and safeguarding, including online and digital safety
- iv. Working in partnership with the DfE and the Internet Service Provider and Abbey IT Manager to ensure systems to protect pupils are reviewed and improved
- v. Receiving reports of online safety incidents and creating a log of incidents to inform future online safety developments
- vi. Reporting to Senior Leadership Team/Headteacher.
- vii. Liaising with the nominated member of the governing body and the Headteacher to provide an annual report on safeguarding, which includes online safety
- viii. Co-ordinating the training and workshops for pupils, staff, Governors and parents to improve understanding of all aspects of online safety
- ix. Keeping up to date on current online safety issues and guidance issued by relevant organisations, including the ISI, the Local Authority, CEOP (Child Exploitation and Online Protection), Childnet International, NSPCC, and the Bi-Borough Safeguarding Partnership.

4.4 IT Manager/Technical Staff

The Abbey IT Manager is responsible for ensuring:

- i. That the School's technical infrastructure is secure and is not open to misuse or malicious attack.
- ii. That the School meets required online safety technical requirements and any relevant body online safety policy/guidance that may apply
- iii. The Abbey IT Manager formally meets with the DSL on a half-termly basis
- iv. That users may only access the networks and devices through a properly enforced password protection policy
- v. This Online Safety Policy, together with the School's approach to filtering and monitoring is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person
- vi. That they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- vii. That the use of the network/internet/Virtual Learning Environment/remote access/Email is regularly monitored in order that any misuse/attempted misuse can be reported to the Headteacher or the DSL for investigation/ action/ sanction.
 - a. That monitoring software/systems are implemented and updated as agreed in School policies.
- viii. Ensure the School's IT system is reviewed regularly with regard to security and that virus protection is installed and updated regularly

4.5 Staff

School staff are expected to:

- i. Read and follow the provisions of this Policy
- ii. Read and Agree to the Acceptable Use of IT Policy/Agreement (Staff and Governors)
- iii. Attend training sessions organised by the School to promote online safety
- iv. As with all issues of safety, staff are encouraged to create a talking and listening culture, in order to address any online safety issues which may arise in classrooms on a daily basis.
- v. Report to the DSL (in respect of pupils) or the Headteacher (in respect of other members of staff) if they become aware of misuse or attempted misuse of Digital Technology within the School

4.6 Pupils

Pupils are expected to:

- i. Read and follow the provisions in this policy.
- ii. Follow the School's Acceptable Use Guidance for pupils relating to the use of digital technology and accessing the School Wi-fi
- iii. Exercise their responsibility to speak out when they believe that the school's systems are being abused in any way

4.7 Parents

The School believes that it is essential for parents, guardians and carers to be fully involved with promoting online safety both in and outside of school. We regularly consult and discuss online safety with parents, guardians and carers to reinforce the importance of children being safe online.

It is important for parents and carers to be aware of what their children are being asked to do online, including the sites the school will ask them to access and who they will be asked to interact with online. They are therefore advised to:

- i. Read any School online safety guidance for parents that is circulated from time to time
- ii. Attend Online Safety sessions and training sessions organised by the School.
- iii. Read the School AUP and discuss its implications with their children.

5. EDUCATION AND TRAINING

5.1 Staff: awareness and training

- New teaching staff receive information on online safety and acceptable use as part of their induction.
- All teaching staff receive regular information and training on online safety issues in the form of targeted training and internal briefings, and are made aware of their individual responsibilities relating to the safeguarding of children within the context of online safety. This includes updated information regarding online filtering and monitoring responsibilities and procedures in the school.
- Staff training in the school is logged centrally.
- All staff working with children are responsible for demonstrating, promoting and supporting safe behaviours in their classrooms and following school online safety procedures. When children use school computers, staff should make sure children are fully aware of the agreement they are making to follow the school's acceptable use guidelines.
- Teaching staff are encouraged to incorporate online safety activities and awareness within their subject areas and through a culture of talking about issues as they arise. They should know what to do in the event of misuse of technology by any member of the school community.
- All incidents relating to online safety should be reported to the DSL.

5.2 Pupils: Online safety in the curriculum

The School delivers age, and stage of development-, appropriate online education through PSHE, assemblies, discussion, talks and the academic curriculum. These are planned and delivered using relevant guidance, tools and resources. This education aims to ensure that all pupils develop the underpinning knowledge and behaviours needed to navigate the online world safely, in a way which suits their age and ability. Teaching staff help pupils achieve this by reinforcing the School's fundamental values.

The curriculum focuses on the following:

- The school provides opportunities to teach about online safety within a range of curriculum areas and IT lessons, as well as informally when opportunities arise.
- At age-appropriate (and stage-of-development-appropriate) levels, and usually via PSHE, pupils are taught to look after their own online safety.
- Enable pupils to understand what acceptable and unacceptable online behaviour looks like
- Raise awareness of the possible online risks and help pupils make informed decisions about how to act and respond
- Reinforce to all pupils the importance of knowing how, when and where

they can seek support if they are concerned or upset by something they see or experience online

- Provide opportunities for pupils, parents and staff to have access to educational workshops, lectures and resources on the all aspects of online e- safety
- Recognise the consequences of inappropriate online behaviour in line with the school's Behaviour Policy but also on their own digital footprint
- Supporting pupils to understand and follow this Policy and the pupil guidance which may be issued by the school regarding the acceptable use of digital technology and online safety
- At age-appropriate points, pupils are taught about recognising online sexual exploitation, stalking and grooming, the risks, and of their duty to report any such instances they or their peers come across. Pupils can report concerns to the DSL (who is the Online Safety Lead) and indeed any member of staff at the school.
- Pupils are also taught about relevant laws applicable to using the internet; such as data protection and intellectual property. Pupils are taught about respecting other people's information and images.
- Pupils should be aware of the impact of cyber-bullying and know how to seek help if they are affected by these issues (see also the school's Anti-bullying Policy, which describes the preventative measures and the procedures that will be followed when the school discovers cases of bullying). Pupils should approach the DSL who is the school's Online Safety Lead or other members of staff as well as parents, peers for advice or help if they experience problems when using the internet and related technologies.
- Special one-off events and awareness days are held to raise the profile of online safety, namely on Safer Internet Day

5.3 Pupils: Vulnerable Pupils

- The School is aware that some pupils are considered to be more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.
- The School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable pupils.
- The School schools will seek input from specialist staff as appropriate, including the SENCO.

6. CYBERBULLYING

The School, as with any other form of bullying, takes Cyberbullying, very seriously. Information about specific strategies or programmes in place to prevent and tackle bullying is set out in the School's S03 Behaviour, Discipline and Exclusions Policy and its S22 Anti-Bullying Policy. The anonymity that can come with using the internet can sometimes make people feel safe to say and do hurtful things that they otherwise would not do in person. It is made very clear to members of the School community what is expected of them in terms of respecting their peers, members of the public and staff, and any intentional breach of this will result in disciplinary action.

If an allegation of bullying does come up, the School will:

- Take it seriously
- Act as quickly as possible to establish the facts. It may be necessary to examine School systems and logs or contact the service provider to identify the bully
- Record and report the incident
- Provide support and reassurance to the victim and support the perpetrator via the individual School's S03 Behaviour, Discipline and Exclusions Policy

7. THE THREAT OF ONLINE RADICALISATION

The internet and the use of social media in particular has become a major way to communicate with others, especially young people, which has provided access for like-minded people to create an online community and confirm extreme beliefs such as extreme ideological views or the use of violence to solve problems. In line with Prevent guidance, protecting children from the risk of radicalisation, the School has a number of measures in place to ensure that children are safe from terrorist and extremist material when accessing the internet in school, and to help prevent the use of social media for this purpose:

- Website filtering and monitoring is in place to help prevent access to terrorist and extremist material and social networking sites such as Facebook, Instagram or X/Twitter by pupils
- Pupils, parents and staff are educated in safe use of social media and the risks posed by on-line activity, including from extremist and terrorist groups.

Further details on how social media is used to promote extremism and radicalisation can be found on the Educate Against Hate website (www.educateagainsthate.com), which is designed to equip schools and college leaders, teachers and parents with the information, tools and resources they need to recognise and address extremism and radicalisation in young people, including in online issues.

8. RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

All members of the School community will be made aware of the reporting procedure for online safety and safeguarding concerns regarding pupil welfare, including: breaches of filtering, youth produced sexual imagery (sexting), upskirting, cyberbullying, sexual harassment and illegal content. For staff, this is done through the school's online safeguarding system, MyConcern. Pupils can raise a concern directly with any trusted adult and parents can raise a concern by contacting Chloe McNeely, DSL, Deputy Head and Online Safety Lead. The school requires staff, parents, carers and pupils to work in partnership to resolve online safety issues.

All members of the community must respect confidentiality and the need to follow the official school procedures for reporting concerns. For further detailed information, the Safeguarding Policy (S11), Parent Complaint Procedure (S04), Low Level Safeguarding Concerns Policy (S11b) and Whistleblowing Policy (S52) can be found on the school website.

After any investigations are completed, the school will debrief, identify lessons learnt and

implement any policy or curriculum changes as required.

If the school is unsure how to proceed with an incident or concern, the DSL will seek advice from the Local Authority Safeguarding Partnership. Where there is suspicion that illegal activity has taken place, the school will contact the Local Authority Safeguarding Partnership or the Police using 101, or 999 if there is immediate danger or risk of harm.

Any allegations regarding a member of staff's online conduct will be referred to the Headteacher and discussed with the DSL/Online Safety Lead and the LADO (Local Authority Designated Officer) if necessary. Appropriate action will be taken in accordance with the Staff Code of Conduct. Staff can raise concerns about a staff member's conduct by completing a report on Confide.

When made aware of concerns involving consensual and non-consensual sharing of nudes and semi-nude images and/or videos by children, staff are advised to:

- Report any concerns to the DSL immediately.
- Never view, copy, print, share, store or save the imagery, or ask a child to share or download it – this may be illegal. If staff have already viewed the imagery by accident, this will be immediately reported to the DSL.
- Not delete the imagery or ask the child to delete it.
- Not say or do anything to blame or shame any children involved.
- Explain to child(ren) involved that they will report the issue to the DSL and reassure them that they will receive appropriate support and help.
- Not ask the child or children involved in the incident to disclose information regarding the imagery and not share information about the incident with other members of staff, the child(ren) involved or their, or other, parents and/or carers. This is the responsibility of the DSL.

The DSL will respond to the concerns as set out in the non-statutory UKCIS guidance: [Sharing nudes and semi-nudes: advice for education settings working with children and young people - GOV.UK \(www.gov.uk\)](https://www.gov.uk/guidance/sharing-nudes-and-semi-nudes-advice-for-education-settings-working-with-children-and-young-people)

For further details regarding the procedures for responding to specific online incidents or concerns, please contact the DSL/Online Safety Lead.

9. MONITORING AND FILTERING

The School will ensure that appropriate filtering and monitoring systems are in place when pupils and staff access school systems and internet provision, so that exposure to any risks can be reasonably limited. Filtering and monitoring are both important parts of safeguarding pupils and staff from potentially harmful and inappropriate online material, but must function without unreasonably impacting teaching and learning, in line with the DfE [filtering and monitoring standards](#) which were updated in March 2025.

9.1 We review our approach to filtering and monitoring regularly and assess the effectiveness of the current provision, any gaps, and the specific safeguarding needs of pupils (their age ranges, those who are at greater risk of harm for example those with SEND, or those with English as an Additional Language (EAL)

and staff. This happens annually (at the very least), or more often if circumstances dictate, such as when:

- a safeguarding risk is identified
- there is a change in working practice, like remote access or BYOD (bring your own device)
- new technology is introduced
- Any checks to the School's filtering provision are completed and recorded as part of the filtering and monitoring review process.

9.2 The Governors have overall strategic responsibility for meeting this requirement, and they have assigned day to day responsibility for the following to the Headteacher and the Abbey Head of ICT:

- procuring filtering and monitoring systems
- reviewing the effectiveness of the School's provision
- overseeing reports

They must also ensure that all staff:

- are appropriately trained for their role
- understand that it is everyone's responsibility to keep the online environment safe, including the effective use of filtering and monitoring
- follow the Staff Code of Conduct, all policies, processes and procedures
- act on reports and concerns, and record them appropriately

9.3 The DSL and Online Safety Lead has the lead responsibility for safeguarding and online safety, which includes overseeing and acting on:

- filtering and monitoring reports
- safeguarding concerns
- checks to filtering and monitoring systems

9.4 The IT Support Department has the technical responsibility for:

- maintaining filtering and monitoring systems
- providing filtering and monitoring reports
- completing actions following concerns or checks to systems

It is important to be able to identify individuals who might be trying to access unsuitable or illegal material so they can be supported by appropriate staff, such as the senior leadership team or the designated safeguarding lead. The School therefore reserves the right to regularly monitor and filter an employee's/pupil's use of the internet, social media and e-mail systems when at work or when using School electronic equipment. Such monitoring/filtering includes the right to read e-mails sent or received on electronic equipment provided by the School or view photographic images captured on electronic equipment provided by the School to check that the use by employees is in accordance with this policy.

9.5 All staff need to be aware of reporting mechanisms for safeguarding and technical concerns. They must report if:

- they witness or suspect unsuitable material has been accessed
- they can access unsuitable material

- they are teaching topics which could create unusual activity on the filtering logs
- there is failure in the software or abuse of the system
- there are perceived unreasonable restrictions that affect teaching and learning or administrative tasks
- they notice abbreviations or misspellings that allow access to restricted material

9.6 The Board of Governors support the Senior Leadership Team to review the effectiveness of monitoring strategies and reporting process. Any incidents that are picked up, are acted on with urgency and outcomes are recorded. Incidents could be of a malicious, technical, or safeguarding nature. Staff know that in the first instance, they report their concerns to the DSL.

9.7 If it is discovered that any of the systems are being abused and/or that the terms of this Policy are being infringed, disciplinary action may be taken in accordance with the provisions of the School's disciplinary policies and procedures.

9.8 Filtering

- The school uses LightSpeed Relay for webfiltering and reporting; e.g. blocking sites which can be categorised as: pornography, racial hatred, extremism, gaming and sites of an illegal nature.
- 365/Azure intelligent language filter works across 365 Apps and Email.
- Microsoft Defender for endpoint anti-virus is installed on all staff/student devices – this works as a filter and blocker both in and out of School.
- The School filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

9.9 Monitoring

- The School will appropriately monitor internet use on all School owned or provided internet enabled devices. This is achieved by all devices being individually registered on our closed networks.
- Pupils are not left alone with electronic devices. All pupils and staff have individual logons, allowing tracking and monitoring of internet use.
- The School has a clear procedure for responding to concerns identified via monitoring approaches: To monitor device and internet use the school are using a product called Lightspeed. The DSL and Headteacher have access to the online portal to view reports and alerts and the system will report immediately via an email to the DSL and Headteacher if specific searches or words have been used. The DSL reviews any concerns flagged by the reports weekly. Any pupil concerns will be followed up by the DSL. Behaviour and Consequences procedures will be followed as appropriate. Any concerns regarding staff internet searches will be passed by the DSL to the Headteacher.
- At a granular level, within School, Network deep packet analysis is monitored by Logrhythm
- All users will be informed that use of School systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

10. ONLINE SAFETY REVIEW

The DSL will regularly review the School's Online Safety Provision and Education

as part of the annual Safeguarding Audit and may use tools such as Online 360 Degree Safe (www.360safe.org.uk) as part of such a review.

11. SECURITY AND MANAGEMENT OF INFORMATION SYSTEMS

Westminster Abbey is responsible for reviewing and managing the security of the computers and Internet networks and takes the protection of School data and personal protection of our School community very seriously. This means protecting the School network, as far as is practicably possible, against viruses, hackers and other external security threats. The Abbey ICT department will review the security of the School information systems and users regularly and virus protection software will be updated regularly at least annually, (or more regularly if circumstances dictate).

Some safeguards that the School takes to secure our computer systems are:

- Advising staff that all personal data sent over the Internet should be encrypted
- Making sure that unapproved software/apps are not downloaded to any School devices. Alerts will be set up to warn users of this.
- Files held on the School network will be regularly checked for viruses
- The use of secure user logins and passwords to access the School network will be enforced.
- Portable media containing school data or programmes will not be taken off-site.
- Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT will be immediately reported to the IT team.

For more information on data protection in the School please refer to the S06 Data Protection Policy.

12. EMAILS

The School uses email internally for staff and pupils, and externally for contacting parents, and is an essential part of School communication. It is also used to enhance the curriculum by:

- Initiating contact and projects with other schools nationally and internationally
- Providing immediate feedback on work, and requests for support where it is needed

Staff and pupils should be aware that School email accounts should only be used for School-related matters, ie for staff to contact parents, pupils, other members of staff and other professionals for work purposes. This is important for confidentiality. The School has the right to monitor emails and their contents but will only do so if it feels there is reason to.

12.1 Staff Use of Email and the internet

Staff should be aware of the following when using emails in the School:

- Staff should only use official School-provided email accounts to communicate with pupils, parents or carers. Personal Email accounts must not be used to contact any of these groups.
- The School permits the incidental personal use of email, the internet, social media and related types of electronic communication and information, and electronic equipment by an employee as long as it is

kept to a minimum and takes place substantially out of normal working hours, this is particularly important for resident staff during their time off duty.

- Staff should be aware that all their personal interactions (email and internet) on a School device are logged, and may be monitored.
- Use must not interfere with an employee's work commitments, or those of others. If it is discovered that excessive periods of time have been spent on the internet or other electronic media provided by the School, either in, or outside, working hours disciplinary action may be taken and internet access or use of electronic equipment may be withdrawn without notice at the discretion of the Headteacher.
- Emails sent from School accounts should be professionally and carefully written. Staff are always representing the School and should take this into account when entering into any email communications
- Where possible, staff should avoid 'replying to all' or blindly forwarding emails they have received. Be selective in your email use.
- Staff must tell their manager or a member of the Senior Leadership Team if they receive any offensive, threatening or unsuitable Emails either from within the school or from an external account. They should not attempt to deal with this themselves.
- The forwarding of chain messages is not permitted in the School.
- Using photographic material of any kind to bully, harass or intimidate others will not be permitted and will constitute a serious breach of discipline and may lead to dismissal.

12.2 Pupil Use of Email

Pupils should be aware of the following when using email in school, and will be taught to follow these guidelines through the IT curriculum and in any instance where email is being used within the curriculum or in class:

- In school, pupils should only use School-approved email accounts
- Pupils are only able to email to approved external addresses provided by parents or guardians and to school email addresses on a separate school server to the rest of the abbey.
- Excessive social emailing will be restricted
- Pupils should tell a member of staff if they receive any offensive, threatening or unsuitable emails either from within the school or from an external account. They should not attempt to deal with this themselves
- Pupils must be careful not to reveal any personal information over Email or arrange to meet up with anyone who they have met online without specific permission from an adult in charge

Pupils will be educated through the ICT and PSHE curriculum to identify spam, phishing and virus Emails and attachments that could cause harm to the School network or their personal account or wellbeing.

13. SAFE USE OF DIGITAL AND VIDEO IMAGES OF PUPILS

The development of digital imaging technologies has created significant benefits to learning, allowing staff and pupils instant use of images that they have recorded

themselves or downloaded from the internet. However, staff, parents, guardians or carers and pupils need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying, stalking or grooming to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term.

When using digital images, staff will inform and educate pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet (e.g., on social networking sites). The school is also mindful of the digital footprint that we are creating for the pupils due to live streaming and other events which are broadcast on television and works to support our pupils to cope with this exposure.

13.1 The School Website

The School considers the school's website to be a useful tool for communicating our ethos and practice to the wider community. It is also a valuable resource for parents, pupils, and staff for keeping up to date with school and School news and events, celebrating school and School-wide achievements and personal achievements, and promoting school projects.

Any information published on the website will comply with good practice guidance on the use of such images and be carefully considered in terms of safety for the School community, copyrights and privacy policies. No personal information on staff or pupils will be published, and details for contacting the School will be for the relevant school office only.

13.2 Safe Use of a Pupil's Digital Images and Data

Parents who accept a place for their child at the school agree in the parental contract to the school's using anonymous photographs and video footage of their child. It is made clear that these images and footage may be used in external news or publicity material for the Choir School or the Abbey.

Published images do not identify pupils or put them at risk of being identified unless they or their parents/carers consent, in which case pupils may be identified by their first name only. An exception to the stipulation that children may not be named refers to those publications that are distributed internally and to parents, where a pupil's full name may be used.

The school has a specific policy regarding the use and storage of images of children, refer to S48 Use and Storage of Images of Children Policy

13.2.1 By Parents

- Parents and others are welcome to take digital images and videos of their children at school events for their own personal use, provided that the license for the event allows, with consideration and courtesy for cast members or performers on stage and the comfort of others. Flash photography can disturb others in the audience, or

even cause distress for those with medical conditions; the School therefore asks that it is not used at indoor events

- Parents are asked not to take photographs of other pupils, except incidentally as part of a group shot, without the prior agreement of that pupil's parents, and publish them on any social media or otherwise publish those images or videos
- Parents should take care taken when taking photos or videos to ensure that pupils are appropriately dressed and are not participating in activities that might bring the individuals or the school into disrepute (they should not be filmed backstage during productions or in changing rooms).
- The School does not however agree to any such photographs or videos being used for any other purpose.
- The School reserves the right to refuse or withdraw permission to film or take photographs (at a specific event or more generally), from any parent who does not follow these guidelines, or is otherwise reasonably felt to be making inappropriate images
- Parents are reminded that copyright issues may prevent the School from permitting the filming or recording of some plays and concerts. The School will print a reminder in the programme or make an announcement at the start of the performance of events where issues of copyright apply.

13.2.3 By Pupils

- The use of cameras or filming equipment (including on mobile phones or mobile action cameras, such as Go Pro cameras) is not allowed in toilets, washing or changing areas, nor should photography or filming equipment be used by pupils in a manner that may offend or cause upset.
- Pupils must not take, use, share, publish or distribute images of others without their permission.
- The School recognises that consensual and non-consensual sharing of nudes and semi-nude images and/or videos (also known as youth produced/involved sexual imagery or "sexting") by/of pupils can be a safeguarding issue; all concerns will be reported to and dealt with by the DSL (or deputy). Creating and sharing nudes and semi-nudes of under-18s (including those created and shared with consent) is illegal which makes responding to incidents complex. (For further information, please see the Safeguarding Policy.)
- The misuse of images, cameras or filming equipment by pupils in a way that breaches this policy, or any other School policy is always taken seriously, and will be dealt with under the relevant policy as appropriate.

13.2.3 By the School

- Staff and volunteers are allowed to take digital and video images to support educational aims, but must follow this policy concerning the sharing, distribution and publication of those images.
- Staff are encouraged to use School issued equipment for the purposes of taking photographs/stills or video footage of pupils. Personal devices may be used if there is no other option, provided:

- a) the image taken is 'appropriate' and is in accordance with the School's Storing and Use of Images Policy
- b) the image is removed from the device within 48 hours. Any such use should always be transparent and staff should be aware of those pupils for whom consent has not been given. The resultant files from such recording or taking of photographs must be stored in accordance with the School's procedures on School equipment.
- c) Consent has been requested from a senior member of staff

13.3 Complaints regarding the Misuse of Digital Images or Video

Parents should follow the standard school complaints procedure if they have a concern or complaint regarding the misuse of photographs/images/videos published by the school. Please refer to our Concerns and Complaints policy, which can be found on the School website, for more information on the steps to take when making a complaint. Any issues or sanctions will be dealt with in line with the Safeguarding Policy.

Misuse of images/videos in any form by pupils and others, will be dealt with in accordance with the school's Behaviour Policy and the Anti-bullying Policy according to the type of incident. Should there be a case of pupils sharing nudes and semi-nudes of under-18s, which is illegal even with the individual's consent, the matter will be immediately referred to the DSL and the Headteacher.

The school will complain to the Press Complaints Council (PCC) if the outside media fail to follow the appropriate code of practice for the protection of young people.

14. SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

The term social media may include (but is not limited to): personal publishing tools including blogs, wikis, social networking sites, video/photo sharing sites, online gaming, bulletin boards, chat rooms and instant messaging. These online forums are the more obvious sources of inappropriate and harmful behaviour and where pupils are potentially more vulnerable to content, contact and conduct behavioural issues. It is important that we educate pupils so that they can make their own informed decisions and take responsibility for their conduct online. There are various restrictions on the use of these sites in school that apply to both pupils and staff.

14.1 Expectations

- The expectations regarding positive, safe and responsible use of social media applies to all members of the School community. The school will control pupil and staff access to social media whilst using school provided devices and systems on site.
- All members of the School community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.
- Concerns regarding the online conduct of any member of the School

community on social media, should be reported to the Headteacher and will be managed in accordance with our Anti-Bullying, Behaviour, and Safeguarding Policies, and Staff Code of Conduct.

14.2 Staff Personal Use of Social Media

- The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities. Further guidelines are found in the Staff Code of Conduct.

14.3 Pupils' Personal Use of Social Media

- Safe and appropriate use of social media will be taught to pupils as part of an embedded and progressive education approach, via age-appropriate sites and resources.
- Pupils are expected not to engage in threatening, hurtful or defamatory online behaviour on social media platforms, in interactive online games or in the metaverse.
- Any concerns regarding pupils' use of social media, both at home and at School, will be dealt with in accordance with existing School policies including anti-bullying and behaviour. Concerns will also be raised with parents/carers as appropriate, particularly when concerning underage use of social media sites or tools.

14.4 Official School Use of Social Media

- The official use of social media sites, by the School, only takes place with clear educational or community engagement objectives, with specific intended outcomes.
- Official school social media channels have been set up as distinct and dedicated social media sites or accounts for educational or engagement purposes only. Official social media sites are suitably protected and, where possible, run and/or linked to/from the school website.
- Official social media use will be conducted in line with existing policies, including: Anti-Bullying, Data Protection, Safeguarding and the Staff Code of Conduct.
- Images and film of the boys may also be used on the Abbey social media websites. These are also official social media channels run in a similar way to those used by the school.

15. USE OF SCHOOL AND PERSONAL MOBILE PHONES AND DEVICES

While mobile phones and personal communication devices are commonplace today, their use and the responsibility for using them should not be taken lightly. Some issues surrounding the possession of these devices are they:

- Can make pupils and staff more vulnerable to cyberbullying
- Can be used to access inappropriate internet material
- Can be a distraction in the classroom
- Are valuable items that could be stolen, damaged, or lost
- Have integrated cameras, which can lead to child protection, bullying

and data protection issues.

The Abbey and School have separate networks set up for staff and pupils. No personally owned devices are allowed to be connected to the school's wireless network, unless using the Visitor wifi.

Residential staff have access to a separate network from the school and Abbey, and all staff residential devices will be separately registered with Abbey IT systems.

15.1 Use by Staff

- Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.
- School devices assigned to a member of staff as part of their role must have a password or device lock so that unauthorised people cannot access the content. Staff should only use the school device which is allocated to them for school work. When they are not using a device staff should ensure that it is locked to prevent unauthorised access.
- The school devices/cameras may be used for official photographs under the direction of the Headteacher. These photographs must only be downloaded using the school's computers and not onto a personal, private computer. Please refer to the Staff Code of Conduct for further details.
- Under no circumstances may staff contact a pupil or parent, guardian or carer using a personal telephone number, email address, social media or messaging system.
- It should be noted that wherever possible, staff will use School-owned devices to capture images or videos, including live streaming. However, staff may use personal mobile devices to take photographs of pupils for social media purposes, PROVIDED THEY COMPLY WITH any relevant School information security policy and that ALL images are only saved onto the relevant School's shared drive.
- Personal mobile phones may be used in dedicated staff areas or in class and teaching rooms only if the children are not present, or in the event of needing to use the authenticator application.
- Computing devices and wearables connected to the school network must always use updated software to safeguard against critical zero-day security vulnerabilities.
- Staff should not accept mobile phone calls during a lesson or when they are with children. The only exception to this is if the Headteacher or DSL calls a staff member (usually only on Sports Days or on school trips, or if the School Office calls in similar circumstances). These calls will only be made in unusual or emergency (safeguarding) situations.
- Staff are advised to ensure that Bluetooth or other forms of communication, such as 'airdrop', are hidden or disabled during lesson times.
- If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or have committed a criminal offence, the

police will be contacted.

- The School accepts no responsibility for, nor provides insurance against, theft, loss or damage of any employee's personal property, including electronic equipment. All such equipment is brought onto the School site at the owner's risk.

15.2 Use by Pupils

15.2.1 Personal Devices

- Pupils at Westminster Abbey Choir School are not permitted to bring personal mobile devices or smart technology onto the school site, including the dormitories, unless for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs.
- If pupils bring in their mobile phones or other digital devices to school, these must be handed into the a member of staff on duty on arrival. It will then be signed into the register of personal property looked after by staff and locked away. The mobile phones/device will then be returned to the pupils when they leave the school site with their parents/carers or to Form V students when leaving if travelling independently. The School will not take responsibility for personal devices that have been lost, stolen, or damaged.
- The school recognizes the fact that many children now have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access increases the risk that some children, whilst at school, are able to sexually harass, bully, and control others via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups), and view and share pornography and other harmful content.
- The School recognizes that pupils are likely to have personal mobile and smart technology in their homes. Where pupils have smart phones at home, parents are responsible for ensuring that they have age-appropriate content filtering configured in the phone settings.
- These requirements apply to phones and all devices that communicate over the internet, including smartwatches and other wearable technology.
- The school recognizes that mobile devices are sometimes used by pupils for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs. Where a pupil needs to use a mobile device for such purposes, the pupil's parents or carers should arrange a meeting with the Headteacher and Head of Learning Support to agree how the school can appropriately support such use. The Head of Learning Support will then inform the pupil's teachers, the DSL, the Abbey Head of ICT and other relevant members of staff about how the pupil will use the device at school.
- Pupils should immediately report, to the DSL/the Online Safety Lead or another member of staff, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- The School expects pupils to think carefully before they post any

information online including liking and/or disliking and/or retweeting (or the equivalent) any post or other element of social media. Content posted should not be able to be deemed inappropriate or offensive, or likely to cause embarrassment to the individual or others.

- Pupils must report any accidental access to materials of a violent or sexual nature directly to the DSL/Online Safety Lead or another member of staff. Deliberate access to any inappropriate materials by a pupil will lead to the incident being recorded on their file and will be dealt with under the School's Behaviour, Discipline & Exclusions Policy. Pupils should be aware that all internet usage via the School's systems is monitored.
- The school recognizes that a number of pupils have access to an old mobile phone in order to listen to music or audio books at bedtime. This is only allowed if the phone is not able to make or receive calls or access the Abbey wifi. Similarly, pupils are only allowed to use kindle devices which cannot also access the wider world wide web.

15.2.2 Policy Breaches

- Any concerns regarding learners use of mobile technology or policy breaches will be dealt with in accordance with our existing policies, including anti-bullying, safeguarding and behaviour, discipline & exclusions.
- If deemed necessary, pupils mobile phones or devices may be searched by a member of the leadership team with the authority of the Headteacher, please see the Anti-bullying Policy and the Behaviour, Discipline & Exclusions Policy for further details. Content may be deleted or requested to be deleted if it contravenes our policies.
- Searches of mobile phone or personal devices will be carried out in accordance with the DfE 'Searching, Screening and Confiscation' guidance: [Searching, screening and confiscation in schools - GOV.UK](#) updated July 2023, as outlined in the School's Searches – Guidance and Protocol document.
- Appropriate sanctions and/or pastoral/welfare support will be implemented in line with our Behaviour, Discipline & Exclusions Policy.
- Concerns regarding policy breaches by learners will be shared with parents/carers as appropriate.
- Where there is a concern that a child is at risk of harm, we will respond in line with our safeguarding policy.
- If there is suspicion that material on a learner's personal device or mobile phone may be illegal, or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

15.2.3 School devices

- All pupils are assigned a School login (email address) for use on our network and to facilitate cloud resources. Access is via a login, which is password protected. This official email service may be regarded as

safe and secure, and must only be used for School work, assignments, research and projects. Pupils should be aware that all digital communication is monitored.

- Anti-virus and firewall protection is used within the School domain. Spam emails, certain attachments and websites will be blocked automatically by the email system. If this causes problems for School work such as assignments, research and projects pupils should speak to their teacher, who will contact the Abbey IT Team.

16 LIVE STREAMING & TELEVISION BROADCASTS

The nature of the Abbey Choir School means that there will be events at the Abbey, involving the pupils, which are live streamed or broadcast on television. Parents will be asked to consent to this when pupils join the choir school.

For all other events where the School decides to permit the live streaming of an event or performance, or for educational purposes, the School will seek the prior consent of parents or pupils (where applicable) to such live streaming, and any subsequent online accessibility to the performance.

17 MANAGEMENT OF APPLICATIONS WHICH RECORD CHILDREN'S PROGRESS (DATA AND IMAGES)

The schools use applications such as iSAMS and Excel to track pupils progress and share appropriate information with parents and carers (this list is not exhaustive). The Headteacher is ultimately responsible for the security of any data or images held of children. As such, they will ensure that tracking systems are appropriately risk assessed by the Abbey's Head of ICT prior to use, and that they are used in accordance with GDPR and data protection legislation

To safeguard data:

- only School-approved apps will be used to access any pupil details, data and images, and these require secure sign ins, passwords and often two-factor authentication.
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
- parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.

18 MANAGING EMERGING TECHNOLOGIES

Technology is progressing rapidly, and with the introduction of Artificial Intelligence (AI), new technologies are constantly emerging. The School assesses the potential risks of any new technologies before permitting their use in schools, carefully weighing these up with the potential educational advantages they may offer. The School may inject AI into their practices, and by doing so, stay at the forefront of innovation, proactively monitoring and keeping abreast of emerging technologies. This approach allows the School to promptly devise and implement suitable strategies to navigate the ever-changing technological

landscape. The school will have due regard to the DfE guidance [Generative AI: product safety expectations](#) for the filtering and monitoring of generative AI.

The school recognizes that AI may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. Westminster Abbey Choir School will treat any use of AI to bully pupils in line with our Anti-Bullying and Behaviour, Discipline & Exclusion policies.

19 PROTECTING PERSONAL DATA

The School takes its compliance with the Data Protection Act 2018 seriously. Personal data will be recorded, processed, transferred and made available online in accordance with General Data Protection Regulations (GDPR) and Data Protection legislation. Full information can be found in the Abbey Privacy Policy, available on the Abbey Website.

20 BREACHES OF POLICY BY EMPLOYEES

Staff should refer to the School's Staff Code of Conduct which sets out the full expectations for staff regarding Online Safety and Internet Use, and the Acceptable Use of IT. It details the repercussions that may follow if these standards are not followed.

A breach of this policy may be treated as misconduct and as such will be dealt with in accordance with the School's Disciplinary policies and procedures. The School reserves the right to contact the Police or other outside agency, as appropriate.

Where an employee wishes to complain about email, internet, social media, electronic images or related electronic communication, or electronic equipment use by another member of staff, they should inform the Headteacher. A complaint by an employee will be dealt with in a timely and appropriate manner in accordance with the provisions of the School's Whistleblowing Policy.

If a complaint against an employee is made by a pupil or parent concerning a breach of this policy the matter will be dealt with in accordance with the School's Concerns and Complaints Policy received from Parents.

If a breach of this policy raises a safeguarding concern the matter will be dealt with in accordance with the School's Safeguarding Policy.

21 VISITORS' USE OF MOBILE AND SMART TECHNOLOGY

Visitors, including volunteers and contractors, who are on site for regular or extended periods of time are expected to use mobile and smart technology in accordance with our acceptable use guidance, and other associated policies, including the safeguarding policies. Please note:

- Visitors wifi is available to visitors but this is only accessible via a password whilst on the school site.
- Members of staff are expected to challenge visitors if they have concerns about their use of mobile and smart technology and will inform the DSL or IT

Services Manager of any breaches of our policy.

22 COMPLAINTS

As with all issues of safety in school, if a member of staff, a pupil or a parent, guardian or carer has a complaint or concern relating to online safety, prompt action will be taken to deal with it. Complaints should be addressed to the DSL in the first instance, who will undertake an immediate investigation and liaise with the Leadership Team and any members of staff or pupils involved. Please see the School Complaints Procedure for further information.

APPENDIX 1: INTERNET ACCESS AND ELECTRONIC SAFETY IN BOARDING

All of the rules and procedures contained within the school's Online-Safety policy apply fully during the formal school day; however, there are a few additions and exceptions which apply within the boarding department after formal school hours.

GENERAL GUIDANCE - All Boarding pupils are subject to the school Online Safety Policy at all times.

Pupils at Westminster Abbey Choir School are not permitted to bring their own mobile devices or smart technology onto the school site including the Boarding House, unless for medical purposes or as an adjustment to assist pupils who have disabilities or special educational needs.

If pupils bring in their mobile phones or other digital devices to school, these must be handed into a member of staff on duty on arrival. It will then be signed into the register of personal property looked after by staff and locked away. The mobile phones/device will then be returned to the pupils when they leave the school site with their parents/carers or Form V if they are travelling independently. The School will not take responsibility for personal devices that have been lost, stolen, or damaged.

Pupils will have supervised access to school computers when on site in school and in the Boarding House. Pupil access to the internet will be via a dedicated pupil network managed by the Abbey IT Department and overseen in school by the Deputy Headteacher.

The School network is protected by internet safety filters and firewalls. It would be usual that pupil network access is terminated at 20.50 each night and enabled from 07.30.

Pupils are forbidden from:

- Downloading music/film which breaches copyright laws
- Accessing gambling sites
- Using unauthorized file-sharing sites
- Using a proxy server with the intention of by-passing the College's 'safe' internet connection
- No pupil may make a recording or take an image of another pupil without their prior consent.
- Pupils must NEVER use a camera facility in private areas within boarding (e.g. bedrooms or bathrooms).

APPENDIX 2: SOURCES OF INFORMATION FOR SCHOOLS AND PARENTS TO KEEP CHILDREN SAFE ONLINE

(from KCSIE 2025, Annex B) (The following list is not exhaustive but should provide a useful starting point).

There is a wealth of information available to support schools and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point:

ADVICE FOR GOVERNING BODIES/PROPRIETORS AND SENIOR LEADERS

- [Childnet](#) provide guidance for schools on cyberbullying
- [Educateagainsthate](#) provides practical advice and support on protecting children from extremism and radicalisation
- [London Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [NSPCC](#) provides advice on all aspects of a school or college's online safety arrangements
- [Safer recruitment consortium](#) "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- [Searching screening and confiscation](#) is departmental advice for schools on searching children and confiscating items such as mobile phones
- [South West Grid for Learning](#) provides advice on all aspects of a school or college's online safety arrangements
- [Use of social media for online radicalisation](#) - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an [Online Safety Audit Tool](#) to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) [Online safety guidance if you own or manage an online platform](#) provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk.
- Department for Digital, Culture, Media & Sport (DCMS) [A business guide for protecting children on your online platform](#) provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse.

SUPPORT FOR CHILDREN

- [Childline](#) for free and confidential advice
- [UK Safer Internet Centre](#) to report and remove harmful online content
- [CEOP](#) for advice on making a report about online abuse

PARENTAL SUPPORT

- [Childnet](#) offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- [Commonsensemedia](#) provide independent reviews, age ratings, & other information about all types of media for children and their parents
- [Government advice](#) about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- [Internet Matters](#) provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- [London Grid for Learning](#) provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- [Stopitnow](#) resource from [The Lucy Faithfull School](#) can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- [National Crime Agency/CEOP Thinkuknow](#) provides support for parents and carers to keep their children safe online
- [Net-aware](#) provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- [Parentzone](#) provides help for parents and carers on how to keep their children safe online
- [Parent info](#) from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- [Talking to your child about online sexual harassment: A guide for parents](#) – This is the Children's Commissioner's parent guide on talking to your children about online sexual harassment
- [UK Safer Internet Centre](#) provide tips, advice, guides and other resources to help keep children safe online

REMOTE EDUCATION, VIRTUAL LESSONS AND LIVE STREAMING

- [Case studies](#) on remote education practice are available for schools to learn from each other
- [Departmental guidance on safeguarding and remote education](#) including planning remote education strategies and teaching remotely
- [London Grid for Learning](#) guidance, including platform specific advice
- [National cybersecurity centre](#) guidance on choosing, configuring and deploying video conferencing.