



S18: PUPIL ACCEPTABLE USE POLICY **FOR THE INTERNET AND EMAIL**

Reviewed: Education and Policy Committee

Approved: Full Governing Body

Approved Date: December 2024

Next Review Date: December 2025

CONTENTS

INTRODUCTION 3

 Why do we need an acceptable use policy? 4

 What are the potential dangers? 4

 What are the legal and ethical issues?..... 5

APPLICABILITY OF THIS AUP 6

PROTECTION OF PUPILS FROM UNSUITABLE MATERIAL ON THE INTERNET . 6

PROTECTION OF PUPILS FROM UNSOLICITED EMAIL CONTACT 6

“CYBER BULLYING” AND “SEXTING” 6

SOCIAL NETWORKING..... 6

CODE OF CONDUCT 7

SANCTIONS FOR BREACHES OF THE AUP..... 7

DISCLAIMER..... 7

SOURCES..... 7

APPENDIX A – INTERNET ACCESS AND ELECTRONIC SAFETY IN BOARDING,
GUIDANCE FROM BOARDING HANDBOOK.....9

APPENDIX B – WESTMINSTER ABBEY CHOIR SCHOOL PUPIL ICT ACCEPTABLE USE
POLICY.....10

INTRODUCTION

This policy outlines an acceptable code of conduct for the use of the IT and systems within Westminster Abbey Choir School.

It is designed to provide a framework for the safe and appropriate use of the internet, balancing the desirability of pupils having full access to resources with the need to protect them from unacceptable material.

Westminster Abbey Choir School recognises 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 our 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 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 and young people. The harm might range from sending hurtful or abusive texts and emails, to enticing children and young people to engage in sexually harmful conversations or actions online, webcam filming, photography or face-to-face meetings.

Educating all members of Westminster Abbey Choir School's 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 at 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.

Westminster Abbey Choir School is conscious of its additional responsibilities to monitor the use of Digital Technology by its boarding pupils. The Designated Safeguarding Lead has joint 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 A.

This policy and our requirements for the Acceptable Use of IT within Westminster Abbey Choir 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.

Why do we need an acceptable use policy?

There are advantages and disadvantages associated with the use of the internet, some of which are described in this document, along with advice about how to overcome them.

Advantages

The internet offers access to a wealth of information and resources that can enrich learning and independent study. It provides:

- Opportunities for world-wide communication
- Opportunities for the development of independent learning and research skills
- Cultural, social and leisure information
- A range of support services.

Disadvantages

There is the potential for misuse of the technology, including pupils gaining access to unsuitable material.

There is no overall control and no censorship of the internet. Users must beware that there are no defined standards for publication of material and what is acceptable to some will be unacceptable to others. This may be due to choice of language or images, standards of expression or cultural and social differences.

Material on the internet varies hugely in quality: some material is biased, inaccurate or misleading (deliberately or unintentionally). Internet users need to beware of the issues of quality and veracity, exercising caution and judgement in their use of what they find.

The internet is dynamic and material can be changed in seconds. It is not safe to assume that what was available yesterday will be the same today or even whether it will be there at all. New information is added constantly and other information disappears.

Pupils need to be protected from obscene material, information relating to the misuse of drugs, the promotion of violence, intolerance, racism, extreme social views and so on. Schools are also now required to take measures to protect pupils from radicalisation and extreme political views.

What are the potential dangers?

Westminster Abbey Choir School acknowledges the provisions of KCSIE (2024) which state: '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 and ever evolving, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful material, for example pornography, fake news, racist or radical and extremist views
- **Contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults,
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm: for example making, sending and receiving explicit images, or online bullying, and
- **Commerce:** being exposed to risks such as online gambling, inappropriate advertising, phishing and or financial scams

What are the legal and ethical issues?

There are a number of laws applicable to the use of the internet including the Obscenity Acts of 1959 and 1964, the Protection of Children Act 1978, the Indecent Displays Act 1981, the Criminal Justice Act 1988 and the Children Act 1989 and 2004. The use of a computer system without permission or for a purpose not agreed by the school could constitute a criminal offence under the Computer Misuse Act 1990. Laws relating to copyright, libel, obscenity or incitement to racial or political hatred are applicable too.

The school and (therefore the Abbey) has the right and a duty to monitor pupils' use of the internet to prevent unlawful or inappropriate use in line with the Education (Independent School Standards) made under section 94 of the Education and Skills Act (2008). Furthermore, very significant responsibilities in this regard are placed on schools under Keeping Children Safe in Education (KCSIE) September 2024. KCSIE makes it clear that such safeguarding responsibilities override concerns about data protection.

The school has a responsibility to protect the pupils in its care. Parents expect the school to promote high standards in relation to the use of computers, the internet and e-safety and to develop the same levels of responsibility in pupils in this area as in any other.

The possibility of inappropriate use of the internet by pupils is something that needs to be understood by teachers and other staff, all of whom may come into contact with the problem. Teachers may be faced with accidental access to unsuitable material (or may encounter pupils attempting to access such material). In such circumstances staff should report the matter immediately to the Headteacher or to one of the Abbey's IT team.

All users are reminded that the possession of certain types of unsuitable material can lead to prosecution.

APPLICABILITY OF THIS AUP

The AUP applies to all pupils; use of the Computer Room signifies understanding and acceptance of the AUP.

Members of staff ensure pupils under their supervision adhere to the AUP.

PROTECTION OF PUPILS FROM UNSUITABLE MATERIAL ON THE INTERNET

All school networks accessible by the pupils have LightSpeed Relay filtering software installed. This filters the internet content accessed by the boys, blocking inappropriate sites and preventing use of social networking sites. Web sites can also be blocked manually if necessary. They also use 365/Azure intelligent language filter across 365 Apps and email.

Any pupil finding themselves feeling uncomfortable or upset by anything they discover on the internet should report the concern to a member of staff immediately.

PROTECTION OF PUPILS FROM UNSOLICITED EMAIL CONTACT

Each pupil has their own email account. All accounts are protected by industry standard anti-spam and anti-virus software. The Abbey uses 365/Azure intelligent language filter across 365 Apps and email and reserves the right to monitor pupils' use of email in order to detect abuse, bullying or unsafe practice, in line with standard NMS 8 and 15 of the National Minimum Standards for Boarding Schools.

Pupils are not permitted to give their email address to anyone without first checking with a member of staff. The E-mail system is set so that safe addresses must be registered with the IT department.

“CYBER BULLYING” AND “SEXTING”

Implicit in the school's responsibility to protect its pupils is the need to prevent bullying and deal with any incidents of it. This includes so-called cyber bullying, harassment and/or sexting whereby ICT (especially the internet, email or portable devices) is misused to cause unhappiness. The school's policies on Safeguarding, Anti-Bullying and Behaviour, Discipline & Exclusions are applicable in such cases.

SOCIAL NETWORKING

Social networking web sites such as Facebook, Twitter, Instagram etc. have become popular amongst children of secondary school age. The majority of such sites prohibit registration by those under 13, and preparatory schools have traditionally blocked access to them. However, given that pupils are likely to register upon leaving the school (or from home before they leave, possibly without their parents' knowledge or consent) it is felt to be more useful to educate final year pupils in the safe use and pros and cons of such web sites, as well as their potential dangers. Pupils may then be allowed some supervised access to online social networks during their free time during their final term once they have reached the age of 13. Their

parents are informed of this practice and receive a letter containing suggestions about how to help their children to get the best out of the internet safely.

Staff users of social networking web sites may not make or accept requests for the “friendship” of current or former pupils until they are adults. Thereafter, they are strongly advised not to engage in online friendship with any former pupils other than on a strictly professional basis, and then only once a former pupil is above school age.

PUPIL ICT ACCEPTABLE USE POLICY

The age of pupils makes it unrealistic to expect them to understand and retain the entire contents of this document. Instead pupils read and sign an ICT Acceptable Use Policy (Appendix B), the policy is counter-signed by their parents. The AUP is also published in the Computer Room. This is thoroughly explained to and discussed with pupils.

SANCTIONS FOR BREACHES OF THE AUP

For minor breaches of the AUP pupils may have their access to IT restricted for a defined period. Other sanctions for breaches will be in line with those detailed in the school’s policy on Behaviour, Discipline and Exclusions.

DISCLAIMER

Neither the school nor the filtering software can guarantee 100% safety from inappropriate material. Pupils are aware of their incumbent responsibilities in the context of the trusting community in which we live and work to uphold the Code of Conduct and report breaches – whether accidental or otherwise – to a member of staff immediately.

SOURCES

This policy draws on information published by:

- the Department for Education (www.education.gov.uk) including the National Minimum Standards for Boarding Schools (2022) and Keeping Children Safe in Education (KCSIE 2024)
- the Boarding Schools’ Association (www.boarding.org.uk)
- CEOP – the Child Exploitation and Online Protection Centre
- SWGfL – Southwest Grid for Learning
- LGFL – London Grid for Learning

APPENDIX A – INTERNET ACCESS AND ELECTRONIC SAFETY IN BOARDING, GUIDANCE FROM BOARDING HANDBOOK

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 in to the Headteacher on arrival. The mobile phones/device will then be returned to the pupils when they leave the school site with their parents/carers. 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 Head.

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).

Name of pupil:

When using the school's ICT facilities and accessing the internet in school, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break school rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Download or install software
- Use any inappropriate language when communicating online, including in emails
- Share any semi-nude or nude images, videos or livestreams, even if I have the consent of the person or people in the photo/video
- Share my password with others or log in to the school's network using someone else's details
- Bully other people
- Use AI tools and generative chatbots (such as ChatGPT or Google Bard):
 - During assessments, including internal and external assessments, and coursework
 - To present AI-generated text or imagery as my own work
- I understand that the school will monitor the websites I visit and my use of the school's ICT facilities and systems.
- I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.
- I know that I can get in touch with [Childline](#).
- I will always use the school's ICT systems and internet responsibly.
- I understand that the school can discipline me if I do certain unacceptable things online, even if I'm not in school when I do them.
- In school, I know that online games may only be played on Wednesdays (as directed), and Saturdays and Sundays after tea.
- I will keep the computer room tidy: will put rubbish in the bin and will not leave anything behind.
- I will not put bring food or drinks in to the computer room.
- I will save paper and ink by only printing what I need.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the school's ICT systems and internet. I agree to the conditions set out above for pupils using the school's ICT systems and internet, and for using personal electronic devices in school, and will make sure my child understands these.

Signed (parent/carer):

Date: