BISHOP WORDSWORTH'S SCHOOL

ICT POLICY

Definitions:

1. 'Parent(s)' includes guardian(s) or any person who has parental responsibility for the pupil or who has care of the pupil.

2. 'Is to', 'are to' and 'must' are obligatory. 'Should' is not obligatory but is best practice and is to be adhered to unless non-compliance can be justified.

AIMS

1. To enable students to use ICT safely and confidently.

2. To provide the opportunity for a varied use of ICT across the curriculum as resources and timetable allow, so that these skills are maintained, used in context and enhanced.

3. To continue to develop the ICT skills and competencies of all staff by providing appropriate training in order to ensure that the facilities are exploited appropriately to enhance teaching.

4. To provide rules on acceptable use of all ICT, including social media, by staff and students.

5. To ensure students are protected from online risks outlined in KCSIE (content, contact, conduct, commerce)

6. To protect Bishop Wordsworth's School ('the School') from legal risks.

7. To clarify ownership of intellectual property.

USE OF ICT IN SCHOOL

8. ICT is used for a wide variety of tasks in school. Some of the main ones for staff (aside from its use in preparing and teaching lesson content) are: to record registration and lesson attendance; to record details of staff appraisal (using BromCom); to record and view safe-guarding issues (using CPOMS); to complete report-writing (using BromCom) and for recording details relating to Sixth Form Mentoring (using MS Teams); to set homework (using MS Teams). Staff also use BromCom to access information about pupil, parents and colleagues in the course of their professional duties.

9. Staff have access to the school network at home. Staff and students have access to a licenced copy of Office 365 which includes files and emails stored on the cloud via Outlook and OneDrive, as well as Teams.

10. All departments must have an ICT-based record-keeping system to enable staff to readily access performance and other data so that pupil progress can be easily tracked to help them achieve their potential. Periodically this data will be submitted centrally to the Assistant Head using BromCom marksheets.

ACCEPTABLE USE OF ICT AND E-SAFETY

11. Acceptable Use is covered by Annex A.

12. E-Safety is covered at Annex B.

13. Data protection is covered in the Data Protection Policy.

14. Students in Year 7 are to be taught about the acceptable use of ICT via their induction lessons as part of their Maths lessons during the first half of term. New students are to

have induction on acceptable use of ICT. Acceptable use and e-safety will also be reviewed through the PHRSE programme.

15. Staff are to have regular reminders about acceptable use and are to receive training on e-safety and what should be done to reduce the risk of exposure to radicalisation/ extremism to themselves and to students, particularly through social media.

INTELLECTUAL PROPERTY RIGHTS

16. All programs, software, documents (of any format), etc produced for the School remain the property of the School.

17. Any member of staff who opens or maintains any social media outlets for the School (X, Facebook, Instagram, Linkedin etc) as a proxy owner does so on behalf of the School which remains the owner of the outlet.

MONITORING AND EVALUATION

18. Use of ICT resources within School is monitored and recorded by the Network Manager and/or ICT Technician in order to determine the most appropriate allocation of these resources.

19. Content filtering is used to identify inappropriate activity by staff and students as outlined in Annex A.

20. Staff training needs are to be identified by the Director of ICT and the Assistant Head i/c CPD and form part of the INSET provision within the School.

21. The Director of ICT and the Network Manager are to evaluate ICT developments, provision, the Acceptable Use Policy at Annex A and the e-safety Policy at Annex B.

22. This Policy was first adopted on 9th October 2007. The most recent 3 years' review history is below:

17th November 2020	Minor updates
16th November 2021	Minor updates
5th March 2024	Online safety and other minor updates

Annexes:

A. Acceptable Use of ICT.
B. E-Safety Policy.

ANNEX A TO
ICT POLICY

ACCEPTABLE USE OF ICT

INTRODUCTION

1. The purpose of this document is to provide clear guidelines for staff and students regarding what is and is not considered appropriate and safe use of the School's ICT facilities and to set out the sanctions that may be employed should these not be followed.

2. Any reference in this Policy to accessing the Internet includes but is not limited to the use of computers (PC, laptop, tablet…), smartphones and any other device that allows the user to access the Internet.

MEASURES

3. In order to provide an Acceptable Use Policy for ICT and the Internet, the School is to adopt certain measures to promote safe use and to reduce the risk of exposure to online harms including illegal, inappropriate or harmful content including radicalisation/extremism:

a. **Use of Filtering System.** Currently the School uses web-filtering provided and maintained by South West Grid for Learning which can be modified as requested by subject teachers e.g. for religious education. The School also uses NetSupport DNA to monitor and report potential Safeguarding issues arising from staff or pupil usage of the Internet and SENSO to monitor and report on Teams communication.

b. **Education & Training.** All new students and staff are to receive formal induction in the use of the school ICT facilities and how to be aware of the risks posed by the online activity of extremist and terrorist groups.

c. **Acceptable Use Policy – Staff.** The Acceptable Use Policy for staff is at Paragraphs 6 to 9 below and all staff are to be made aware of it during induction and are to abide by it.

d. **Acceptable Use Policy – Students.** The "Acceptable use of ICT and the Internet" agreement (at Appendix 1) is electronically signed by parents when their child joins Yrs7-11 (as part of the Digital Welcome Pack issued via Insight). Joiners in the Sixth Form sign their own agreement.

e. **Supervision.** Wherever possible ICT staff or teaching staff should supervise the use of school computers.

f. **Reporting System.** Studentsare to be encouraged to report to the ICT staff any dubious material that they find. Currently the ICT staff filter out the relevant material and this is picked up by the School's filtering which is updated daily.

g. **Penalties for Misuse – Students.** Misuse or abuse of the school ICT facilities will result in loss of ICT privileges and/or disciplinary action such as:

(1) A ban, temporary or permanent, on the use of the Internet facilities at School.

(2) A letter informing parents of the nature of the breach of rules.

(3) Appropriate sanctions and restrictions placed on access to School facilities to be decided by the Head of Year/Head of Department.

(4) Any other action decided by the Head or Governors of the School.

h. **Penalties for Misuse – Staff.** Misuse or abuse of the school ICT facilities will be dealt with by the Head or Governors.

THE ACCEPTABLE USE POLICY (AUP)

4. The AUP consists of 4 components:

   a. Aims of the AUP.

   b. AUP for staff.

   c. AUP for Pupils.

   d. Letter to parents.

5. **Aims of the Acceptable Use Policy.** The aims are:

   a. To allow all users to access and use the Internet for educational purposes, including e-mail and World Wide Web facilities

   b. To cover School activities such as: individual research, preparation of lessons, project work, homework assignments, communicating with others in the School community, or those outside the community where relevant.

   c. To provide a mechanism by which staff and students are protected whilst connected to the School ICT network from sites, information and individuals which would undermine the principles and aims of the School, and to reduce the risk of exposure to online harms.

   d. To provide rules which are consistent and in agreement with the Data Protection Policy and other relevant legislation including the 'Prevent Duty' and KCSIE.

   e. To provide rules which are consistent with the acceptable procedures commonly used on the Internet, including those associated with netiquette.

6. **Acceptable Use Policy Staff – School Network.**

   a. The School's ICT Suites may not be block-booked more than one term in advance. Exceptions to this would be for lessons requiring regular access to ICT (e.g. for NEA, Art, EPQ, MFL, etc.) that need to be planned well in advance.

   b. Staff must not make changes to the School's ICT system by adding or removing any hardware, software or peripheral applications without the knowledge of the Network Manager or ICT Technician. Data is to be protected in accordance with the Data Protection Policy.

   c. Any materials produced by a member of staff whilst employed by the School that are specifically for use in fulfilling their role will remain the property of the School even if/when the member of staff is no longer employed by the school. Staff who are leaving the School may take copies of any material they have produced, but must not permanently remove the material from the school network.

   d. Staff must ensure that the ICT suites are left tidy at the end of their lesson and that the equipment is left in a working condition. All damage, etc. must be reported to the ICT staff as soon as possible.

   e. Staff are to make every effort to ensure that all students have followed the AUP.

   f. Staff are to immediately report any incident which breaches the AUP to the ICT Staff.

   g. Staff are advised that their use of the school internet is (remotely) monitored at all times.

7. **Acceptable Use Policy Staff – Security and Online Safety.**

a. Staff are to log-out of the School network when they leave a room to which pupils have open access and to ensure the projector is switched off. This is especially important if applications allowing access to confidential information (e.g. BromCom, CPOMS, etc.) have been used. If the staff member will be returning to the room within minutes the PC may be locked instead.

b. If staff are viewing BromCom and/or CPOMS in a classroom they must make sure that the projector is turned off, or the image frozen/muted so that confidential information is never displayed.

c. Staff must ensure that any photographs that they wish to be posted on the School's website directly or on any social media:

(1) Do not include students whose parents have requested that their children do not appear in such publicity material.

(2) Do not include the names of the students in such a way that an individual pupil can be identified.

d. Staff must exercise care when using any material that is copyrighted especially on items that appear on the School's website. They must always seek permission from the owner and, if in doubt or unable to obtain permission, must not use the material (outside of accepted fair use).

e. Staff must not view, upload or download any material which is likely to be unsuitable for students unless it relates specifically to legitimate course content. This applies to any material that contains inappropriate sexual content, is of a violent, racist, or dangerous nature or that appears to support or endorse extremist or terrorist groups.

f. Inappropriate language is not to be used in any form of electronic communication.

g. Passwords are not to be disclosed to anyone as this will undermine the security of the system.

h. Passwords must meet the requirements of and be changed in accordance with the Data Protection Policy.

i. Staff are not to publish any content which could result in actions for defamation, discrimination, breaches of copyright, data protection or other claim for damages. For example material of an illegal, sexual, extremist or offensive nature that may bring the School into disrepute.

j. Staff must take every reasonable precaution to ensure that students are not exposed to online harms including, but not limited to, radicalisation or terrorism, promotion of self-harm and suicide, misogyny and racism.

k. Staff must be aware of commercial risks both individually and on the behalf of students. These include online gambling, phishing and financial scams. Emails received which staff believe fall into this category should be reported to the Network Manager.

l. Staff must be aware that anything posted on the internet could become publicly available as a result of changes to privacy settings made by providers, or through security breaches.

m. In some lessons, such as PHRSE, it might be deemed acceptable to show material that might otherwise be considered inappropriate. In such cases, staff are to consider the benefits of showing such material against the possible ramifications. If there is any

doubt about the wisdom of such an action, staff are always to err on the side of caution and should discuss this with department or section heads, or a member of the Leadership Team.

n. It is never appropriate to show any form of pornography in a school context.

o. Staff are strongly advised to avoid accessing student pages on social networking sites to avoid the possibility of viewing inappropriate or potentially illegal materials about underage students.

p. Similarly, staff must avoid viewing student files on portable memory devices (for instance, to find who it belongs to) without an adult witness in case inappropriate or potentially illegal images are viewed.

q. Email communication between staff and students must only be through school email accounts; personal accounts or social media are not to be used.

r. Taking, making, sharing and possessing indecent images and pseudo-photographs of people under 18 is illegal. As 'making' includes opening an attachment, staff must take care when opening email attachments, especially if they are from an unknown source. Any such emails must not be forwarded as this is considered to be 'sharing'.

8. **Acceptable Use Policy Staff – Use of Social Media.** 'Social Media' refers to social networking sites (such as X, Instagram and Facebook), digital media sharing, email and blogs. The following rules and advice are to be followed by staff:

a. Email communication between staff and students must only be via School email accounts and not personal accounts. Alternatively, this could be done via Teams Chat or Posts.

b. Staff must not become 'friends' with currently on-roll students(or any ex-pupil under the age of 18) on social networking sites except through sites specifically set up by/ within the School.

c. Staff must exercise care when posting material on social networking sites – especially if that material can be seen by anyone. Privacy settings must be checked and amended as appropriate.

d. Staff are advised that if their out-of-work activity causes potential embarrassment for the School or detrimentally affects the School's reputation, then the School is entitled to take appropriate disciplinary action. This includes creating fake/imitation accounts and identity theft.

e. Staff must not use the School network for the promotion of personal financial interests, commercial ventures or personal campaigns.

f. Staff must not post material using social media:

(1) During their hours of work, unless this is for legitimate School purposes, e.g. posting school activities on school account feeds.

(2) To discuss or advise on matters relating to the School, staff, students or parents.

(3) That refers to any staff member, pupil, parent or School activity/event unless prior permission has been obtained and agreed with the Head or the posting appears on a School-endorsed website.

(4) That would breach any of the School's policies (for example, those relating to discipline & grievance, equality, freedom of information or harassment and bullying).

(5) That could be deemed to promote or endorse terrorist or extremist groups.

g. Staff are also advised to consider the reputation of the School in any posts or comments on any social media that could be related to the School.

h. Staff must not engage in any form of Cyber Bullying – the use of text messages or web spaces/e-mails/blogs, etc. to either send offensive materials or post them for others to view.

9. **Acceptable Use Policy Staff – Use of Mobile Telephones.** In accordance with the Staff Disciplinary Procedure, Annex C (The Staff Code of Conduct) Appendix 1 Paragraph 4 staff must not use their personal mobile phones to communicate with students via the pupil's personal mobile phones or landlines. If there is a need to contact students on their mobile phone or landline, for instance in an emergency, then this is to be via a school telephone (mobile or landline).

10. **Acceptable Use Policy – Students.** The following rules are to be observed by all students:

a. Students must abide by the student agreement that has been electronically signed by their parents. A copy of the agreement is available to students via Bromcom.

b. Students must only access those services they have been given permission to use.

c. Unless authorised, students must not use the School's computers without supervision.

d. Use of the Internet, during the school day, must be directly related to work.

e. Private use of the Internet in school is only to be undertaken with permission of the ICT staff and as an after-school activity.

f. Students are not to disclose their password to anyone.

g. Students are not to give personal addresses, telephone/fax numbers of any adult working at the school, or any pupils at the school.

h. Students are not to communicate with staff through their personal accounts. They should only do this through their school email or Teams accounts.

i. Students are not to post photographs with names annotated.

j. Before uploading material to the internet, students must obtain permission from the owner. If using material from the internet, pupils must check that they are permitted to do so. If permission is given, the material must be properly identified as someone else's work and acknowledged appropriately. If in doubt, or permission cannot be obtained, they are not to use the material (outside of accepted fair use).

k. Students must not view, upload or download any material which is likely to be unsuitable for pupils or schools unless it specifically relates to legitimate course content at the School. This applies to any material of a violent, dangerous racist nature, or that contains inappropriate sexual content. If they are not sure about specific content they are to seek advice from a teacher.

l. Students must not upload, download or publish material that could be deemed to promote or endorse terrorist or extremist groups.

m. Students are to be taught to always respect the privacy of files of other users. They must not enter the file areas of other pupils or staff.

n. Students are to agree that the ICT technical staff may view any material stored on the school's computers or on media that are used on the school's computers.

o. Students are to be polite and appreciate that other users might have different views than their own. The use of strong language, swearing or aggressive behaviour is not allowed. Students are not to make malicious or derogatory comments on school systems nor on any social media that could bring the School into disrepute or that could be libellous.

p. Students must never deliberately cause damage to any computers, computer systems, networks or software. Furthermore, if they discover any misuse, they must report this immediately to a member of the ICT staff and not divulge it to any other person. Food and beverages are not allowed near the computer systems.

q. Students must not use the School's ICT equipment for any commercial purposes or use their credit cards or banking details on any of the School's computers.

r. Students must not create fake/imitation accounts that purport to represent other people or institutions and must not pose as other students or adults online.

s. Students must not engage in any form of Cyber Bullying or peer-on-peer abuse, i.e. the use of text messages or web spaces/emails/blogs, etc. to either send offensive materials or post them for others to view.

t. Students must not upload or forward any text, image, sound file or video that could humiliate, embarrass or intimidate people as a result of being viewed by a wider audience.

u. Students must be aware that anything posted on the internet could become publicly available as a result of changes to privacy settings made by providers, or through security breaches.

Appendix:

1. Acceptable Use of ICT and the Internet Agreement.

APPENDIX 1 TO
ANNEX A TO
ICT POLICY

ACCEPTABLE USE OF ICT AND THE INTERNET AGREEMENT

Access to the School's computers is provided for the purposes of educational research and learning. The purpose of this agreement is to provide rules for acceptable use of these facilities. Students and parents should carefully read and then sign the following agreements.

STUDENT AGREEMENT

I understand that access to ICT and the Internet provided by Bishop Wordsworth's School must be in support of educational research or learning, and I agree to the following:

- I will use the School's ICT facilities, the Internet, email and MS Teams in a responsible manner at all times including on personal electronic equipment.
- I will ensure that my password access is secure and I will never use the account of another user.
- I will be courteous and respectful, and use appropriate language. I will refrain from using obscene, harassing or abusive language on the computer systems and I will report any cases of such usage against me to my teacher or the ICT staff.
- I will not damage computers, computer systems, software or networks. Furthermore, if I discover any methods of causing such damage I will report them to the ICT staff and I will not demonstrate them to others.
- I accept that ICT staff have the right to access any of my files or email on the School's computers, and that staff may also request access to files on external media and personal electronic equipment that I bring into school.
- I will never knowingly access any sites on the Internet which contain pornographic, racist or violent material, nor will I explore methods of bypassing the school's filtering arrangements.
- I will not access any unauthorised newsgroups, chatrooms or social networking sites or otherwise communicate with unknown persons.
- I will reject any unsuitable materials, dialogues and information received by me.
- I will not use valuable Internet time playing non-educational games.
- I accept responsibility to prevent copyrighted material from entering the School. Therefore I will not download software, games, music, graphics, videos or text materials that are copyrighted. I will not violate any copyright laws by posting or distributing copyrighted material.
- Plagiarism is unacceptable. Therefore I will use any downloaded material in an appropriate manner in assignments, listing its source in a bibliography and clearly specifying any directly quoted material.
- I will not use any school ICT equipment for commercial purposes.
- I will not engage in any activity that promotes or endorses the activities of terrorist or extremist groups.
- I will not produce, either in or out of School, any defamatory material about the School or about a member of the School's community, particularly with regard to my own Web sites or on any social media.
- I will not reveal personal information, including names, addresses, credit card details and telephone numbers of others or myself.
- I will not engage in Cyber Bullying or peer-on-peer abuse – the use of text messages or web spaces/e-mails/blogs etc. to either send offensive materials or post them for others to view.
- I will report any abuse or suspicious communication that I find disturbing to my parents, members of staff, www.ceop.gov.uk or www.thinkuknow.co.uk

If I violate any of the terms of this agreement I understand that I will be denied access to the School's network for a time to be determined by the Headmaster. In addition I may face further disciplinary action or, if appropriate, legal proceedings as determined by the Headmaster and /or Governors. I am aware that each case will be considered on its merits.

PARENTAL AGREEMENT

I hereby acknowledge that I have read the agreement on pupil use of ICT and the Internet and discussed it with my child. I understand that this access is designed for educational purposes. I recognise that, while every effort will be made to monitor pupil use of the Internet, it is impossible for Bishop Wordsworth's School to monitor the use of the system continually and to restrict access to all controversial materials. I further acknowledge that questionable material may be accessed unexpectedly and, therefore, I will not hold the Headmaster or staff of Bishop Wordsworth's School responsible for any such materials acquired from the Internet.

Please tick the Internet Access box on Insight to signify your agreement

ANNEX B TO
ICT POLICY

ONLINE SAFETY POLICY

INTRODUCTION

1. The purpose of this policy is to ensure that students and staff at Bishop Wordsworth's School are able to use communication technologies (the internet, email, mobile phones and other hand-held devices) safely and responsibly, and that children are protected from potentially harmful and inappropriate online material.

2. This document should be read in conjunction with the School's ICT Policy and the sections on Acceptable Use as well the policies on Behaviour and Child Protection.

3. Reference to *inappropriate material* includes such items as: abusive or offensive materials of all types, images/text of a racist or sexual nature, images/text that others perceive to be hurtful

RESPONSIBLE USE

4. Online safety depends on users exercising judgement and common sense when using all types of communication technologies. All users have a responsibility not to compromise the privacy and personal security of themselves and of others.

5. The School's filtering arrangements will block student access to a range of sites accessed via the School's network deemed inappropriate in a school environment, including social networking sites, though it is recognised that there is a fine balance to be struck between regulation of use and enabling users to benefit fully from access to the Internet. However, mobile technologies such as 4G and 5G are harder to regulate and so students must be educated in staying safe and reporting misconduct taking place on these platforms.

6. Mobile phones may be used in school as long as the rules regarding their use are followed. These are specified in Appendix 1 to Annex B of the Behaviour and Discipline Policy: The School Rules).

7. The School's provision of Internet access is intended for educational use only.

8. The School maintains a record of all users granted Internet access via the School network.

9. Staff and students must agree to abide by the Acceptable Use Policy. Parents also electronically sign the Student Agreement via the parent portal.

PROTECTING STAFF AND STUDENTS

10. The breadth of issues classified within online safety is considerable and ever evolving, but can be categorised into four main areas of risk:

a. **Content;** being exposed to illegal, inappropriate or harmful content, for example pornography, fake news, misogyny, self-harm and suicide, anti-Semitism, radicalisation and extremism.

b. **Contact:** being subjected to harmful online interaction with other users, for example, peer to peer pressure, commercial advertising, adults posing as children with the intention to groom or exploit them.

c. **Conduct:** online behaviour that increases the likelihood of harm, or causes harm, such as making, sending or receiving explicit images and online bullying.

d. **Commerce:** Risks such as online gambling, inappropriate advertising, phishing or financial scams.

11. Whilst it is recognised that it may not be possible to guarantee that students will never come into contact with inappropriate materials whilst at School, especially as access to the Internet may not always be directly supervised and as students may access the Internet via their personal mobile devices, the School will take reasonable precautions to ensure student and staff security whilst on site.

12. The Network Manager (or ICT Technician) may permit access to specified websites, to which pupil access is usually denied, as requested by teaching staff.

13. Students will be taught about appropriate and responsible use of all forms of communication technologies at school and at home. They will be made aware of how to ensure they stay safe when using the internet, and of the dangers and possible consequences of careless or irresponsible use, such as the disclosure of personal information on newsgroups and social networking sites, and of all forms of cyber-bullying or peer-on-peer abuse. They will also be made aware that anything posted on the internet could become publicly available as a result of changes to privacy settings made by providers, or through security breaches. This information will be given in tutorials, Year 7 ICT Induction and in PHRSE lessons where applicable, and reinforced in assemblies.

14. Staff safe-guarding training will include online safety for staff and students.

15. All reasonable steps are to be taken to reduce the risks of exposure to staff and students from the online activities of extremist and terrorist groups.

EVALUATING CONTENT AND ASSESSING RISK

16. Methods to identify, assess and minimise risks to pupils will be reviewed regularly.

17. Pupils and staff must immediately report any offensive e-mails to either their teacher or to the Network Manager/ICT Technician.

RESPONSES TO MISUSE, AND SANCTIONS

18. The use and misuse of all forms of communication technologies by students is covered by both the School's Behaviour Policy (and associated sanctions) and the Acceptable Use Policy. This includes creating fake/imitation accounts and identity theft.

19. Incidents of misuse are, in the first instance, to be dealt with by the class teacher. Depending on the severity of the incident, the student may then be passed on to the Section Heads, then to the Network Manager, and/or the Head as appropriate.

20. Where a student has posted inappropriate material on the internet and this can be viewed by others, the School (if it is aware of this) will ask the offending student to remove it as soon as possible. If the student fails to comply, the School may take appropriate disciplinary action.

21. Parents/carers of students who misuse ICT and related technologies will be informed of their child's behaviour, if appropriate.

22. Issues of Child Protection/ Safeguarding must be referred to the Designated Safeguarding Lead (DSL) or their Deputy.

23. Where a member of staff has posted inappropriate material on the internet, including but not limited to creating fake/imitation accounts and identity theft, and this can be viewed by others, the School will ask the offending member of staff to remove it as soon as

possible. If the member of staff fails to comply, the School may take appropriate disciplinary action.

24. Complaints about Staff misuse will be referred to the Head and may lead to actions in accordance with the School's Whistleblowing Policy.