The Bishops' Blue Coat Church of England High School

Online Safety Policy

All of the policies that shape our lives and daily practice at Bishops` are informed by our Christian vision and values: to know, nurture and inspire our students to be the best version of themselves, so that they can live 'Life in all its fullness' (John 10: 10)

Is this policy statutory?	No
Review Period	Annual
Approved	February 2025
Committee	Students

Contents

Statement of Intent

Our vision statement states that:
The Bishops' Blue Coat Church of England High School is an exciting place to be. We know, nurture, and inspire our community to be the best version of themselves through a better understanding of the Christian faith, and a rich set of opportunities that support and challenge our learners, so they are equipped to succeed. Through their engagement in society at Bishops' and beyond, students make a positive difference through their wise action and a sense of responsibility. Our students' initiative, drive and resilience will enable them to flourish and live 'life in all its fullness.' (John 10:10).

We believe that all people are made in the image of God and are unconditionally loved by God. Everyone is equal and we treat each other with dignity and respect and the safety, protection, and well-being of all in our school community is fundamental. Our school is a place where everyone should be able to flourish in a loving and hospitable community.

2. Aims

Our school aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, and governors.
- Identify and support groups of students that are potentially at greater risk of harm online than others.
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

a. **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
b. **Contact** – being subjected to harmful online interaction with other users, such as 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
c. **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
d. **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Relationships Sex and Health Education (RSHE) Education
- Searching, screening and confiscation

It also refers to the DfE's guidance on Protecting Children from Radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.
The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and Responsibilities

3.1 The Governing Board

The governing board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.
The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring. The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.
The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).
The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.
The governing board must ensure the school has appropriate filtering and monitoring systems in place on school devices and school networks and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The governor who oversees online safety is Chris Woods. All governors will:

- Ensure they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the school's ICT systems and the internet (appendix 1)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school or college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable.

3.2 The Headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.3 The Designated Safeguarding Lead

Details of the school's designated safeguarding lead (DSL) and DDSLs' are set out in our child protection and safeguarding policy, as well as relevant job descriptions.
The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school.
- Working with the headteacher and governing board to review this policy annually and ensure the procedures and implementation are updated and reviewed regularly.
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the Data & Systems Manager to make sure the appropriate systems and processes are in place.
- Working with the headteacher, Data & Systems Manager and other staff, as necessary, to address any online safety issues or incidents.
- Managing all online safety issues and incidents in line with the school's child protection policy
- Ensuring that any online safety incidents are logged (on CPOMS) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face.
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively.

This list is not intended to be exhaustive.

3.4 The Data & Systems Manager

The Data & Systems Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.

This list is not intended to be exhaustive.

3.5 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently

- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 2), and ensuring that students follow the school's terms on acceptable use (appendix 1)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes and being aware of how to report any incidents of those systems or processes failing by alerting the DSL and or DDSL as soon as possible.
- Following the correct procedures by emailing the DSL and network manager with a request with at least two days' notice if they need to temporarily bypass the filtering and monitoring systems for educational purposes outlining the reason why.
- Working with the DSL to ensure that any online safety incidents are logged (on CPOMS) and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy.
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'.
- Ensuring that they use their own personal social media in a responsible manner, including having the maximum-security settings to keep their information secure. Staff who are linked online to the school will ensure that their content does not bring the school or profession into disrepute.
- Following section 19 of the Safeguarding policy in regard to contact with current and former students online.

This list is not intended to be exhaustive.

3.6 Parents/Carers

Parents/carers are expected to:

- Notify a member of staff, the DSL or the headteacher of any concerns or queries regarding this policy
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 1)

Parents/carers can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? – UK Safer Internet Centre
- Hot topics – Childnet International
- Parent resource sheet – Childnet International

3.7 Visitors

Visitors who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (appendix 2).

3.8 Members of the Community

There is a Public Wi-Fi facility available to members of the public in the huddle at weekends. Appendix 3 sets out the applicable acceptable use

4. Educating Students about Online Safety

Students will be taught about online safety as part of the curriculum:
The text below is taken from the National Curriculum computing programmes of study.
It is also taken from the guidance on relationships education, relationships and sex education (RSE) and health education.

All schools have to teach:

- Relationships education and health education in primary schools
- Relationships and sex education and health education in secondary schools

Secondary Schools
In **KS3**, students will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy.
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.

Students in **KS4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity.
- How to report a range of concerns

By the **end of secondary school**, students will know:

- Their rights, responsibilities, and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online.
- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them.
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (e.g. pornography) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence that carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

The safe use of social media and the internet will also be covered in other subjects where relevant.
Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse and some students with SEND.

5. Educating Parents/Carers about Online Safety

The school will raise parents'/carers' awareness of internet safety in letters or other communications home, and in information via our website. This policy will also be shared with parents/carers.
Online safety will also be covered in the half-termly safeguarding newsletter.

The school will let parents/carers know:

- What systems the school uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the school (if anyone) their child will be interacting with online

If parents/carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the DSL and or the Headteacher.
Concerns or queries about this policy can be raised with any member of staff, the DSL or the headteacher.

6. Cyber-Bullying

6.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of 1 person or group by another person or group, where the relationship involves an imbalance of power. (See also the school behaviour policy.)

6.2 Preventing and Addressing Cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.
The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Form teachers will discuss cyber-bullying with their tutor groups through the LIFE programme.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support students, as part of safeguarding training (see section 11 for more detail).
The school also sends information/leaflets on cyber-bullying to parents/carers so they are aware of the signs, how to report it and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining Electronic Devices

The headteacher, PSOs, DDSLs' and the DSL can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, and/or
- Is identified in the school rules as a banned item for which a search can be carried out, and/or
- Is evidence in relation to an offence?
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
- Make an assessment of how urgent the search is, and consider the risk to other students and staff, they will seek advice from the DSL and/ or DDSL's.
- Explain to the pupil why they are being searched, how the search will happen, and give them the opportunity to ask questions about it.

- Seek the pupil's co-operation.

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
Where these is suspicion that a student's electronic device contains indecent material of an under 18-year-old then they will confiscate the device but will not examine it but will contact the Police in line with our Safeguarding policy, page 20.
When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, and/or
- Undermine the safe environment of the school or disrupt teaching, and/or
- Commit an offence.

If inappropriate material is found on the device, it is up to the DSL / DDSL/ headteacher to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
- The pupil and/or the parent/carer refuses to delete the material themselves.

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

Any searching of students will be carried out in line with:

- The DfE's latest guidance on searching, screening and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Behaviour for Learning Policy (BESt)

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure.

6.4 Artificial Intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.
The Bishops' Blue Coat Church of England High School recognises that AI has many uses to help students learn, but 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.
The Bishops' Blue Coat Church of England High School will treat any use of AI to bully students in line with our Dignity and Respect (anti-bullying) and Behaviour for Learning (BESt) policy.
Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used.

The Bishops' Blue Coat Church of England High School recognises that whilst AI can be beneficial to students, it will educate students on the risks of its use in an educational setting and the possible contravention of exam board regulations resulting in malpractice following guidance from the JCQ.

7. Acceptable Use of the Internet in School

All students, parents/carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the school's ICT systems and the internet (appendices 1 and 2). Visitors will be expected to read and agree to the school's terms on acceptable use if relevant. Use of the school's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role. We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above and restrict access through filtering systems where appropriate.
More information is set out in the Acceptable Use Agreements in appendices 1 and 2.

8. Students Using Mobile Devices in School

Electronic device is used to refer to any type of digital device including mobile phones, Smartwatches, Fitbits, iPads/tablets, and earphones/wireless earphones which use the same technologies. Electronic devices which are brought into school must be switched off (NOT placed on silent) and stored out of sight in students' bags during learning time. This means that electronic devices are only permitted during unstructured times. These are before school, break time, lunchtime and after school. Electronic devices must also be off and away between lessons and the sounding of the 'movement' bell as this is also learning time. Such devices must not be kept in students' pockets. If devices are seen, they may be requested and kept in a safe place until the end of the school day. If a student persistently chooses to misuse their electronic device, the Year Leader may consider imposing further limitations on their personal usage.

There are two exceptions to this:

8.1 Permitted Electronic Devices

Some students will need access to electronic devices during a learning activity as is specified in their educational passport or for medical needs.

8.2 Sixth Form Social Area and Sixth Form Lessons

Sixth Form students may use their electronic devices in the classroom when express permission has been given by the teacher. The use of personal electronic devices in one lesson for a specific purpose does not mean 'blanket usage' is then acceptable. Electronic devices are also permitted in the Sixth Form Silent Study Room and the Sixth Form Social Area. Sixth Form students will need to ensure their phones are off and away when not in the Bistro, Sixth Form lessons, Silent Study Room and the Sixth Form Social Area.

8.3 Inappropriate use of Electronic Devices

The way in which students relate to one another online can have a significant impact on the culture at school. Negative interactions online can damage the school's culture and can lead to school feeling like an unsafe place. Even though the online space differs in many ways, the same standards of behaviour are expected online as apply offline. Everyone should be treated with kindness, respect, and dignity.
Inappropriate use of electronic devices can include the following (this list is not exhaustive)

- Device used to target others – child on child abuse (inappropriate online behaviour including bullying, the use of inappropriate language, the soliciting and sharing of nude or semi-nude images and videos, and sexual harassment)
- Device used to photograph or video students during the school day when consent has not been given.
- Device used to photograph or video members of staff.
- Device accesses inappropriate online content (eg gambling or accessing age restricted content)

If there is suspected inappropriate use of electronic devices, then staff will request the device and refer to Pastoral Teams. Staff may examine any data or files on the device where there is a good reason to do so as outlined in section 6.3. They may also delete data or files if they think there is a good reason to do so, unless they are going to give the device to the police. If an electronic device that is prohibited by the school rules has been seized and the member of staff has reasonable grounds to suspect that it contains evidence in relation to an offence, they must give the device to the police as soon as it is reasonably practicable. Material on the device that is suspected to be evidence relevant to an offence, or that is a pornographic image of a child or an extreme pornographic image, should not be deleted prior to giving the device to the police. The Safeguarding Team must be consulted before contacting the police, to guide next steps.

There is no need to have parental consent to search through a young person's mobile phone if it has been requested with consent of the child, or in a lawful 'without consent' search, and is prohibited by the school rules or is reasonably suspected of being, or being likely to be, used to commit an offence or cause personal injury or damage to property. In determining a 'good reason' to examine or erase the data or files the staff member should reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the school rules. If a staff member does not find any material that they suspect is evidence in relation to an offence and decides not to give the device to the police, they can decide whether it is appropriate to delete any files or data from the device or to retain the device as evidence of a breach of school discipline.

Inappropriate use of electronic devices is a serious breach of BESt and will receive a C5 Senior Referral. Students may then be put on monitoring reports where their devices are handed in at the beginning of the school day and returned to the student at the end.

9. Staff Using Work Devices Outside School

All staff members' school devices (e.g. iPads, laptops) have the following centrally managed security measures to ensure safety

- Password-protection.
- Their hard drive is encrypted – this means if the device is lost or stolen, no one can access the files stored on the hard drive by attaching it to a new device
- The device locks if left inactive for a period of time
- Current anti-virus and anti-spyware software
- Operating systems that are up to date by always installing the latest updates
- Work devices must be used solely for work activities. It is the individual member of staff's responsibility to not share the device among family or friends. If staff have any concerns over the security of their device, they must seek advice from Jonathan Price the Data &systems Manager.

10. How the School will Respond to Issues of Misuse

Where a pupil misuses the school's ICT systems or internet, we will follow the procedures set out in our policies on behaviour. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the school's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The school will consider whether incidents that involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

11. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues, including cyber-bullying and the risks of online radicalisation. All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse.
- Children can abuse their peers online through:
  - Abusive, harassing, and misogynistic messages
  - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
  - Sharing of abusive images and pornography, to those who don't want to receive such content.
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element.

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse.
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks.
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term.

The DSL and DDSLs will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills about online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.
More information about safeguarding training is set out in our child protection and safeguarding policy.

12. Monitoring Arrangements

The DSL/ DDSL and PSO's will log behaviour and safeguarding issues related to online safety in CPOMS.

This policy will be reviewed every year by the [DSL and Data & systems Manager]. At every review, the policy will be shared with the governing board. The review (such as the one available here) will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with other policies

This online safety policy is linked to our:
Safeguarding Policy / Cyber Security Policy / Behaviour Policy / Dignity and Respect (anti-bullying) Policy / Staff Code of Conduct / Data Protection Policy / Complaints Policy

13. Appendices

Appendix 1: Acceptable Use Agreement (Staff, governors and volunteers)

THE BISHOPS' BLUE COAT CHURCH OF ENGLAND HIGH SCHOOL

Staff and Volunteer Acceptable Use Policy

(Applies to Staff, Governors and Volunteers)

Appendix to Online Safety Policy

All of the policies that shape our lives and daily practice at Bishops` are informed by our Christian vision and values: to know, nurture and inspire our students to be the best version of themselves, so that they can live 'life in all its fullness' (John 10:10)

Is this Policy Statutory?	No
Review Period	Annual
Date Approved	September 2023
Committee	Full Governors

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

- that school ICT systems and users are protected from accidental or deliberate misuse that could put systems or users at risk that staff are protected from potential risk in their use of ICT in their everyday work.

The school will ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement:

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed e-safety in my work with young people.

School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

For my Professional and Personal Safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.

- I understand that the rules set out in this agreement also apply to use of school ICT systems (eg laptops, email, Remote Access, Office 365, Satchel and IRIS) out of school.

- I understand that the school ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.

- I will respect system security and I will not disclose my password or security information. I will use a 'strong' password.

- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

- I will not disconnect or move any PC, printer or projector. I understand that all such moves are the responsibility of the ICT Support team and will request via the Helpdesk that they undertake any such required move.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language.

- I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role or the school into disrepute.

- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so.

- I will only communicate with pupils and parents using official school systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities (e.g. social networking pupils)

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.

- I understand that data protection policy requires that any staff or student / pupil data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority. Our Data Protection Policy complies with current Data Protection legislation.

Using Personal Digital Devices:

- When I use my personal hand-held/external device (tablets / laptops / mobile phones / USB devices etc) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use.

- When I access personal data from outside of school (via email or Remote Desktop (RDS) or OneDrive) I will ensure that I do so in a secure manner, including securing the device itself with a passcode or password that is not shared with anyone else. I will further ensure that my device is kept up to date with best security practices (antivirus/antimalware programs, system updates, etc.)

- I understand that the school has legal responsibility for the safe and secure

transmission/storage of personal and sensitive data. I understand that the school may therefore take steps to limit or prevent access to such data including email from personally owned devices. I will ensure that personal devices which contain school information i.e. emails are password protected with a secure password for safe use.

Staff (and Volunteer) Acceptable Use Agreement Form:

- I understand that I am responsible for my actions in and out of school:
- I understand that this Acceptable Use Policy applies not only to my work and use of school ICT equipment in school, but also applies to my use of school ICT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action.
- I have read and understand the above and agree to use the school ICT systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines.

Staff / Volunteer Name
Signed
Date

Appendix 2: Acceptable Use Agreement (KS3, KS4 and KS5 students and parents/carers)

THE BISHOPS' BLUE COAT CHURCH OF ENGLAND HIGH SCHOOL

Student Acceptable Use Policy

Appendix to Online Safety Policy

All of the policies that shape our lives and daily practice at Bishops` are informed by our Christian vision and values: to know, nurture and inspire our students to be the best version of themselves, so that they can live 'life in all its fullness' (John 10:10)

Is this Policy Statutory?	No
Review Period	Annual
Date Approved	September 2023
Committee	Full Governors

New technologies have become integral to the lives of children and young people today, both inside and outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone in a safe virtual environment.

This Acceptable Use Policy is intended to ensure:
That young people will be responsible users and stay safe while using the internet and other technologies for educational/recreational use.
That school ICT systems and users are protected from accidental or deliberate misuse that could put systems or users at risk.
The school will ensure that students have good access to ICT to enhance their learning and will, in return, expect students to agree to be responsible users.

Acceptable Use Policy Agreement:
I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety/the safety of others, or to the security of the ICT systems.

I understand that the school will monitor my use of the ICT systems, wireless network, email, and other digital communications.

I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.

I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

I will immediately report any damage or faults involving equipment or software however this may have happened.

I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

I will act as I expect others to act toward me:
I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without permission.

I will be polite and responsible when I communicate electronically with others and will not use strong, aggressive or inappropriate language.

I will not take or distribute images of anyone without their permission

Mobile devices (BYOD):
I will only use my personal mobile device in lessons if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

I understand the risks and will not try to upload, download, or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

I will only use chat and social networking sites (e.g. Edmodo, Instagram, Snapchat, Facebook, Twitter) with permission and at the times that are allowed.

When using the internet and email, I agree that:
Access is a privilege and requires responsible behaviour.

I will not use the school ICT systems for on-line gaming, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so.

I will be aware of "stranger danger" when I am communicating on-line.

I will not disclose or share personal information about myself or others when on-line.

If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

I will immediately report any inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that I am responsible for my actions, both in and out of school:
I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community.

I understand that if I fail to comply with this Acceptable Use Policy Agreement, I may be subject to disciplinary action. This may include loss of access to the school network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

Appendix 3: Acceptable Use Agreement (Public Wi-Fi)

THE BISHOPS' BLUE COAT CHURCH OF ENGLAND HIGH SCHOOL

Public Wi-Fi Acceptable Use Policy

(Public users of the Wi-Fi in the Huddle)

Appendix to the Online Safety Policy

This policy includes our terms for the use of the Bishops' Blue Coat CE High School (Bishops' High School) public Wi-Fi network facility (the Service). The policy exists to allow the public to enjoy free access to the internet in an open environment. By connecting to this Service, you agree to be bound by the terms of this Acceptable Use Policy (the Policy).

Violation of this Policy may result in the suspension or termination of your access to the Service and/or prosecution and/or Bishop' High School co-operating with law enforcement organisations, government agencies, other legal authorities or third parties involved in the investigation of any suspected or alleged criminal or civil offence.

This Policy prohibits the following (each a Prohibited Activity):

- Using the Service in a manner which violates or facilitates the violation of any laws, regulations, or other government requirements in any jurisdiction or the rights of any third party, including using the Service:
  - to harm or attempt to harm minors in any way; o to commit an offence under the Computer Misuse Act 1990 (as amended);
  - in a manner that infringes the rights of others including intellectual property rights (for example by downloading or distributing pirated software, music and films) or the terms of any software license agreements;
  - to access, display, store or transmit any material that is unlawful, harmful, threatening, defamatory, obscene, infringing, harassing or racially or ethnically offensive, or which depicts sexually explicit images;
  - to promote unlawful violence, discrimination based on race, gender, colour, religious belief, sexual orientation, disability; o to carry out any activities which are fraudulent;
  - in connection with any other illegal activities.
- Using the Service in an immoral or improper manner including to make or send offensive, indecent, menacing, nuisance or hoax communications or to cause annoyance, inconvenience or needless anxiety;
- Using the Service to violate the security of a network, service or other system including to gain unauthorised access to computer systems of the Council or of other users, or information held on them. 11 July 2012
- Use of the Service in a manner which may damage Bishops' High School's reputation.
- Using the Service for any activity which adversely affects the ability of other users of the Services or the internet or in breach of any third party policies for acceptable use or any other relevant internet standards (where applicable).
- Using the Service for business purposes or to 'spam' including sending any unsolicited emails and collecting the responses of unsolicited emails.
- Reselling the Service (whether for profit or otherwise). By using this Service you agree and acknowledge that:
- you are fully responsible for all activities and communications in respect of your use of the Services;

- you will not use the Services to carry out any Prohibited Activity;
- you will not cause unnecessary noise and will respect the privacy of other users; and

You further agree to indemnify and keep indemnified Bishops' High School in respect of all losses (including, without limitation, all direct, indirect direct and consequential losses to the fullest extent possible) suffered by Bishops' High School as a result of any failure to comply with this Policy.

Disclaimer

- Bishops' High School does not guarantee that Service will be compatible with your equipment or warrant that the Service will be available at all times, uninterrupted, error-free, or free of viruses or other harmful components, although it shall take reasonable steps to provide the best Service it can.
- Bishops' High School's Service provides a level of web content filtering to exclude racist, violent, pornographic or other offensive content. However, web content filtering is not foolproof and the Council accepts no liability for any data or content that you access or receive via the Service.
- The Service is monitored with a secure log of all use, including websites visited, for the purpose of helping to improve the Service and ensure users abide by the Policy. Bishops' High School will not use any personal information in the log for any other purpose but may disclose such information to other people or organisations where reasonable in relation to the investigation of any suspected or alleged criminal or civil offence and in accordance with the Data Protection Act 1998 and other applicable laws.
- Bishops' High School is not responsible for the privacy or security of your activities and, in particular, urges caution when undertaking financial transactions online. Online financial transactions are carried out at your own risk and Bishops' High School does not accept any liability for any loss of any kind that may arise from the use of the Services in connection with such transactions.
- Bishops' High School is not responsible for the safety, security, configuration or integrity of any of your equipment or data used to access the Services. It is your responsibility to provide adequate security for your equipment, including anti-virus software. Use of the Services with your equipment and data is entirely at your own risk, and Bishops' High School does not accept any liability for any loss of or damage to equipment and data (including, without limitation, indirect and consequential loss) that may arise through the use of the Services.
- Nothing in this Policy shall limit Bishops' High School's liability for fraudulent misrepresentation or death or injury caused by the negligence of Bishops' High School or any of its employees, agents, officers or subcontractors.