



**BISHOP RAWSTORNE**  
Church of England Academy

# Technology Acceptable Use Agreement - Student

*'But the wisdom that comes from heaven is first of all pure; then peace loving, considerate, submissive, full of mercy and good fruit, impartial and sincere'*  
James 3:17

Approval date: **April 2026**  
Approved by: **Deputy Headteacher**  
Next review: **April 2027**

This document and the content contained therein remains the responsibility of the Headteacher, and Governing Body of the Academy. No amendments can be made without their express instruction and they remain the final arbiters in any matters relating to it.

**FORTITER ET FIDELITER**  
*Bravely and Faithfully*

## **Bishop Rawstone Church of England Academy Technology Acceptable Use Agreement – Student Policy**

### **Verse**

“But the wisdom that comes from heaven is first of all pure; then peace loving, considerate, submissive, full of mercy and good fruit, impartial and sincere.”

James 3:17

### **Vision**

“Bishop Rawstone Church of England Academy aspires to cultivate wisdom rooted in Christian Values. It is our vision that all members of our community will experience life in all its fullness, flourishing through dignity, knowledge and understanding, bound together in unity, giving hope and worth to all.”

### **Our Values**

Hope, Service, Compassion, Peace, Wisdom, Fellowship.

Our values are taken from the work of Neville Norcross ‘Christian Values for Church Schools’. Whilst there are many Christian values, we have chosen the six above to complement our commitment to a rich curriculum and outstanding pastoral care.

### **Philosophy**

At Bishop Rawstone Church of England Academy, we believe that access to information and communication technology should support high-quality teaching, learning, and communication in a manner that reflects our Christian values of wisdom, service, and respect. We are committed to ensuring that all use of ICT is safe, purposeful, and responsible. Our Acceptable Use Policy sets out clear expectations that help safeguard individuals, promote digital responsibility, and foster an environment in which technology enhances learning and community life.

### **CODE OF CONDUCT IN OUR CHRISTIAN COMMUNITY**

Our aim is to ensure that you feel happy, safe and secure in your school.

*We believe:*

- that every individual in our community is a unique and valuable creation made in the image of God.
- we all have a right to be considered equal, worthy of respect and esteem.
- we all have a responsibility to treat others as we would like to be treated ourselves.

## **POLICY APPLICATION**

The school's online safety policy reflects the importance it places on the safe use of information systems and electronic communications.

Online safety encompasses not only internet technologies but also electronic communications via mobile phones and games consoles. It highlights the need to educate children and young people about the benefits, risks and responsibilities of using information technology.

- online safety concerns safeguarding children and young people in the digital world.
- online safety emphasises learning to understand and use new technologies in a positive way.
- online safety is less about restriction and more about education about the risks as well as the benefits so we can feel confident online.
- online safety is concerned with supporting children and young people to develop safer online behaviours both in and out of school.

The Internet is an unmanaged, open communications channel. The internet, including email, blogs and social networks all transmit information at low cost. Anyone can send messages, discuss ideas and publish material with little restriction. These features of the Internet make it an invaluable resource used by billions of people every day.

Some of the material on the Internet is published for an adult audience and can include violent and adult content. Information on weapons, crime and racism may also be unsuitable for children and young people to access. Students need to develop critical skills to evaluate online material and learn that publishing personal information could compromise their security and that of others. Schools have a duty of care to enable students to use online systems safely.

It is the responsibility of the school to make it clear to students, staff and visitors that the use of school equipment for inappropriate reasons is "unauthorised", and to ensure a Technology Acceptable Use Agreement is in place.

The rapid development and accessibility of the Internet and technologies such as social networking means that online safety is an ever growing and changing area of interest and concern. The school's online safety policy reflects this by keeping abreast of the vast changes taking place around us.

The school's online safety policy must operate in conjunction with other school policies including Anti-Bullying, Child Protection & Safeguarding and Student Rewards & Sanctions. Online safety is also built into the curriculum.

Please note that for the security of the network, pen drives are no longer acceptable. This includes encrypted pen-drives.

## **WEB-BASED TECHNOLOGIES**

- The Internet provides instant access to a wealth of up-to-the minute information and resources from across the world, which would not ordinarily be available.
- Use of email enables improved communication and facilitates the sharing of data and resources.
- Microsoft 365 (including Teams/Classroom tools) and subject-specific platforms (e.g Sparx, Bedrock and Seneca) provide students with access to resources, assignments and independent learning activities in and out of school.

### UNFORTUNATELY, WITH THIS CAN COME:

- Students might inadvertently access content of an unsavoury, distressing or offensive nature on the Internet or receive inappropriate or distasteful emails.
- Students might receive unwanted or inappropriate emails from unknown senders, or be exposed to abuse, harassment or 'cyber-bullying' via email, text or on social-networking websites and apps, such as Facebook, Twitter and Instagram etc.
- Chat rooms provide cover for unscrupulous individuals to groom children.
- Identify theft – including gaining unauthorised access to accounts on platforms commonly used by young people (e.g., Snapchat, Tiktok, Instagram, WhatsApp and Discord).

## **SOCIAL AND EDUCATIONAL BENEFITS TO BE DERIVED FROM THE UNDERSTANDING AND USE OF E-TECHNOLOGIES:**

- Children and/or young adults are equipped with skills for the future.
- The Internet provides instant access to a wealth of up-to-date information and resources from across the world, which would not be otherwise available.
- The Internet helps to improve children's and/or young adults' reading and research skills.
- Email and the use of some networking areas helps to foster and develop good social and communication skills.
- Bishop Rawstorne Church of England Academy feels that the benefits far outweigh the risks involved so long as users are made aware of the issues and concerns and receive ongoing education in choosing and adopting safe practices and behaviours.
- This policy has been written and focuses on each individual technology available within Bishop Rawstorne Church of England Academy and outlines the procedures in place to protect students and the sanctions to be imposed if these are not adhered to.

## **PROCEDURES FOR USE OF A SHARED NETWORK**

- Users must access the network using their own accounts. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's account or files on the network without permission.
- Software should only be installed by the Network Manager.
- Users must ensure they have adequate virus protection on any machine on which they use removable media before it is used in school.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+alt+del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

## **PROCEDURES FOR USE OF THE INTERNET AND EMAIL**

### **PROCEDURES FOR USE OF ARTIFICIAL INTELLIGENCE (AI) TOOLS (INCLUDING IMAGE-BASED TOOLS SUCH AS GOOGLE LENS):**

AI-enabled tools can support learning when used appropriately, but they can also be used to bypass learning, undermine academic honesty and compromise safeguarding and privacy. Some tools (including image-based question solvers such as Google Lens) are disabled on the school network and devices; however, they may still be accessible outside school.

- Students must not use AI tools (including image-based tools such as Google Lens) to generate answers for classwork, homework, assessments, tests or examinations and then present this work as their own.
- Students must follow teacher instructions about when (if ever) AI tools may be used to support learning and must acknowledge/declare use when required.
- Students must not use AI tools to bypass school filtering, monitoring or other safety controls, or attempt to access blocked services on the school network.
- Students must not upload or share personal data, images of other people, schoolwork containing personal information, or any confidential information into AI tools or services.
- If a student becomes aware that AI tools are being used to cheat, bully, harass, impersonate, or otherwise cause harm, they should report this to a trusted adult or a member of staff immediately.
- All users must sign a 'Technology Acceptable Use Agreement' before access to the Internet and email is permitted in the establishment. All students are reminded regularly to respect other student's personal information/data and to not share it.
- Parental or Carer consent is requested via the student data collection sheet in order for students to be allowed to use the Internet or email.
- Users must access the Internet and email using their own account and not those of another individual. Passwords must remain confidential and no attempt should be made to access another user's email account. If you feel your account details are known by others you should change your password immediately.
- The Internet and email must be used in a reasonable manner adhering to the professional judgment of the supervising member of school staff.
- Students must be supervised at all times when using the Internet and email.
- Procedures for safe Internet use and sanctions are applicable if rules are broken.
- Accidental access to inappropriate material is to be reported to a member of the teaching staff or the Network Manager and a note of the offence recorded and acted upon.
- Internet and email filtering software is installed to restrict access, as far as possible, to inappropriate or offensive content and to reduce the receipt of 'spam,' junk or unwanted correspondence. This is to be reviewed and updated regularly.
- Access to Microsoft 365 is configured with location-based restrictions: sign-ins are limited to the UK and access from outside the UK may be blocked or require additional security checks.
- Internet and email use will be monitored regularly in accordance with data protection legislation.
- Users must be careful when they disclose any information of a personal nature in an email or on the Internet. This includes mobile and home phone numbers, addresses, or anything else which might allow them to be identified.
- All emails sent should be courteous and the formality and tone of the language used appropriate to the reader. Sanctions, appropriate to the case, will be imposed on any users who break this code.

- Bullying, harassment or abuse of any kind via email will not be tolerated. Sanctions, appropriate to the case, will be imposed on any users who break this code.
- If users are bullied, or offensive emails are received, this must be reported immediately to a trusted adult or member of staff within school. Emails received should not be deleted, but kept for investigation purposes.
- Copyright must not be broken.

### **FILE TRANSFER:**

*Files may be taken home or brought into school using the following methods:*

- Attached to emails using students' individual school e-mail accounts.

*Remember - the school uses special filtering software, which prevents you from accessing most unsuitable sites and it also records every attempt you make to hit a site, whether successful or not, when and where you did it and who you are. So remember - every action you take under your account is recorded, and may be accompanied by screenshots and/or recordings of your session.*

### **PROCEDURES FOR USE OF CAMERAS, VIDEO EQUIPMENT AND WEBCAMS:**

- Permission must be obtained from a student's parent or carer before photographs or video footage can be taken.
- Photographs and/or video footage can be downloaded and stored into an appropriate area under the guidance of the Network Manager.
- Any photographs or video footage stored, must be deleted immediately once no longer needed.
- Students and staff must conduct themselves in a polite and respectful manner when representing the school in a video conference or when corresponding via a webcam. The tone and formality of the language used must be appropriate to the audience and situation.

### **PROCEDURES TO ENSURE SAFETY OF THE BISHOP RAWSTORNE CHURCH OF ENGLAND ACADEMY WEBSITE:**

- Website safety is the responsibility of the Network Manager or the designated member of staff.
- All content and images must be approved before being uploaded onto the website prior to it being published.
- The website is checked every term to ensure that no material has been inadvertently posted, which might put students or staff at risk.
- Copyright and intellectual property rights are respected.
- Permission is obtained via the data collection sheet from parents or carers before any images of students can be uploaded onto the website.
- Names are not used to identify individuals portrayed in images uploaded onto the website. Similarly, when a student is mentioned on the website, photographs which might enable this individual to be identified must not appear.
- When photographs to be used on the website are saved, names of individuals should not be used as file names.

**PROCEDURES FOR USING MOBILE PHONES, MP3 PLAYERS, IPODS, IPADS AND OTHER PERSONAL DEVICES:**

- The school is NOT responsible for students' mobile phones, pMP3 players, Tablets or iPods being damaged, lost or stolen. Items are brought to school at your own risk.
- If a mobile phone, MP3 player, tablets or iPod needs to be brought into school, it should be switched off at all times and stored in bags.
- If a mobile phone, MP3 player, tablet or iPod is activated in school, it will be confiscated immediately, recorded and kept in the school safe as per the mobile phone policy. Repeat occurrences will result in students being referred to the Assistant Headteacher, Pastoral Care or Heads of Year.

### **PROCEDURES FOR USING GAMES CONSOLES:**

- The use of games consoles will not be permitted in school at any time. Students may use Kindles as part of literacy developments and other e-reading.

### **IF A STUDENT BREAKS ANY OF THE RULES, THE FOLLOWING MAY HAPPEN:**

- A temporary ban on the use of all computer facilities at school until a discussion takes place with the Curriculum Area Leader of TAC and/or the Assistant Headteacher, Pastoral Care or Heads of Year.
- A ban, temporary or permanent, on the use of the Internet facilities at school.
- Appropriate punishment within the departmental and/or school pastoral systems.
- A letter informing parents what has occurred.
- Any other action decided by the Headteacher and Governors of the school.

### **TRAINING**

- All staff and students to receive regular and up-to-date training via PSHE, computing and within departments for students. INSET provision will be provided for school-based staff. Students will receive age-appropriate online safety information within the school curriculum which focusses on how to stay safe, protect themselves from harm and how to take responsibility for their own online safety and that of others.
- An audit of training needs for all staff to improve their knowledge and expertise in the safe and appropriate use of new technologies is undertaken regularly.

### **ONLINE SAFETY GUIDANCE**

- Online safety guidance is to be displayed in all classrooms.

### **MONITORING AND EVALUATION OF ONLINE SAFETY**

- Review of provision to occur annually to ensure it continues to meet changing technologies and school priorities. The School Council and e-Safety Group are involved with the continued development of online safety at Bishop Rawstorne Church of England Academy.

### **CONCLUDING STATEMENT:**

The procedures in this policy will be subject to ongoing review and modification in order to keep up with advances in the technology at Bishop Rawstorne Church of England Academy. It may be that staff /students might wish to use an emerging technology for which there are currently no procedures in place. The use of emerging technologies will be permitted upon completion and approval of a risk assessment, which will be used to inform future policy updates.

This policy is to be viewed in conjunction with the Anti-Bullying and Safeguarding policies.

**ACCEPTABLE USE AGREEMENT FOR STUDENTS**

The Internet is an invaluable global resource potentially available to anybody with a computer or Internet-enabled device. The network at Bishop Rawstone Church of England Academy will support Internet use and will allow students access to a wide range of information and resources. The Government is committed to use of the Internet in schools as a regular resource to support learning. We are, however, aware that some sites are inaccurate, defamatory, illegal or offensive and the following precautions will be taken when users log on to the Internet in school.

**THE INTERNET**

- Only access those Internet services you have been taught and have permission to use.
- The work/activity on the Internet must be directly related to your schoolwork.
- Always ask permission from the owner before using any material on the Internet or credit the source.
- Always respect the privacy of files of other users (on the Internet and on the school network).
- Never disclose your password and do not lose or forget it.
- Never download, use or upload any proxy sites, applications, games, MP3 files or any other material that is copyrighted.
- Never view, upload or download any material that is likely to be unsuitable for children or for use in the school. This applies to any material of a violent, dangerous, racist or sexual nature. If you are unsure about this or any materials, you must ask the supervising teacher.
- The Headteacher, Network Manager and Computing staff will have the right to view any materials you store on the school's computers, emails you send or receive, websites you view or attempt to view or on disks you use on school computers.
- I will not use AI tools (including image-based tools such as Google Lens) to complete work for me or to avoid learning: I will follow staff instructions about acceptable use, and I understand misuse may be treated as academic dishonesty.

**EMAIL**

- When using e-mail, be polite and appreciate that the other users may have different views than your own. Remember - your e-mails can be printed and passed on to other people - so write it exactly as you would write a letter.
- The use of strong language or aggressive or insulting statements is not allowed.
- Do not state anything on a web page or in an e-mail that could be interpreted as libellous.

Signed: \_\_\_\_\_ (Student) \_\_\_\_\_ (Parent)

Full Name: \_\_\_\_\_ (Student) \_\_\_\_\_ (Parent)

Date: \_\_\_\_\_

**THE NETWORK**

- Users must access the network using their own accounts. These must not be disclosed or shared.
- Users must respect confidentiality and attempts should not be made to access another individual's account or files on the network without permission.
- Software should not be installed without prior permission from the Network Manager responsible for managing the network.
- Users must ensure they have adequate virus protection on any machine on which they use removable media before it is used in school.
- Machines must never be left 'logged on' and unattended. If a machine is to be left for a short while, it must be 'locked.' (Ctrl+Alt+Del followed by 'lock computer').
- Machines must be 'logged off' correctly after use.

**THE INTERNET AND EMAIL**

- Never disclose your password or allow others to use your internet facilities.
- When using the school system, the Headteacher, Network Manager and the Computing staff have the right to view any materials you store on the school's computers, emails you send or receive, websites you view or attempt to view or on disks you use on school computers.

Signed: \_\_\_\_\_

Full Name: \_\_\_\_\_

Date: \_\_\_\_\_

# **BISHOP RAWSTORNE CHURCH OF ENGLAND ACADEMY**

## **ACCEPTABLE USE OF IT**

**THESE RULES HELP KEEP EVERYONE SAFE AND RESPECTFUL OF OTHER USERS**

- **I WILL ONLY ACCESS THE SYSTEM WITH THE ACCOUNT PROVIDED**
- **I WILL NOT ATTEMPT TO ACCESS OTHER PEOPLE'S ACCOUNTS**
- **I WILL NOT USE ICT EQUIPMENT WITHOUT A MEMBER OF STAFF SUPERVISING**
- **I WILL ONLY EMAIL PEOPLE I KNOW FOR WORK/LEARNING PURPOSES**
- **THE MESSAGES I SEND WILL BE POLITE AND RESPONSIBLE**
- **I WILL NEVER GIVE OUT PERSONAL INFORMATION**
- **I WILL REPORT ANY UNPLEASANT MATERIAL OR MESSAGES I SEE OR RECEIVE**
- **I UNDERSTAND ALL COMPUTER USE IS LOGGED AND THERE WILL BE CHECKS AND MONITORING OF MY USE AND THE SITES I VISIT**