Bishop Rawstorne Church of England Academy

Online Safety and Acceptable IT Use Policy

I have come in order that you might have life—life in all its fullness.

John 10:10

Aspire Believe Achieve

This policy 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.

Review date:	**November 2017**
Next review date:	To be reviewed in April 2018 in order to meet General Data Protection Register guidelines that come into place in May 2018
Reviewed by:	**Miss Palmer**

To be reviewed in April 2018 in order to meet General Data Protection Register guidelines that come into place in May 2018

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.

Bishop Rawstorne Church of England Academy needs to protect itself from legal challenge and ensure that staff work within the boundaries of professional behaviour. It is an offence to use email, text or instant messaging (IM) to 'groom' children.

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 ensure an Acceptable Use Policy is in place. Online safety training is an essential element of staff induction and part of an ongoing CPD programme. However, we are aware that a disclaimer is not sufficient to protect from a claim of personal injury and as a school we need to ensure that all reasonable actions have been taken and measures put in place to protect users.

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 Behaviour, Child Protection and Anti-Bullying. online safety must be built into the curriculum.

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.
- Virtual Learning Environments (VLEs) provide students with a platform for personalized and independent learning.

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 hacking Facebook profiles and other social media accounts.

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

- All users must sign an 'Acceptable Use Agreement' before access to the Internet and email is permitted in the establishment.
- 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.
- Internet and email use will be monitored regularly in accordance with the Data Protection Act 1998.
- 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.

PROCDURES FOR USING MOBILE PHONES, PENDRIVES, MP3 PLAYERS, IPODS, IPADS AND OTHER PERSONAL DEVICES:

- The school is NOT responsible for students' mobile phones, pen drives, MP3 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 Senior Leader, 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 Lead Teacher of Computing and/or the Senior Leader, 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 was undertaken at Easter 2014.

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 is to be 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 Safe Guarding policies.

APPENDIX 1

ACCEPTABLE USE AGREEMENT FOR STAFF & STUDENT TEACHERS

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.
- Users may purchase and/or install additional software, from the Internet or otherwise, provided the user complies with all relevant legislation.
- Removable media should be scanned for viruses before being used on a machine connected to the network.
- 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.
- Staff must never allow a student access to the network via their staff account.

THE INTERNET AND EMAIL:

- Never disclose your username or password or allow others to use your Internet facilities.
- When using your school e-mail, be aware that this is for work purposes.
- When using the school system, the Headteacher, Network Manager and the IT 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: _____

APPENDIX 2

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 Rawstorne 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.

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: _____

APPENDIX 3

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**