

Bradford Christian School

Policy statement for e-safety

Aims:

We aim to protect and educate students and staff on their safe and wise use of technology.

To have appropriate mechanisms to intervene and support students and deal effectively with any incident that occurs in school.

To combat the following three areas of e-safety risk

- **content:** being exposed to illegal, inappropriate or harmful material
- **contact:** being subject to a harmful online interaction with other users
- **conduct:** personal online behaviour that increases the likelihood of or causes harm to self or others

The vulnerability of children is a central concern in this policy and foundational is our commitment to our child safeguarding.

Responsibilities:

The policy applies to all members of the school community including: staff, students, parents, visitors, who have access to and are users of the school e-systems both in and out of school, including trips.

In dealing with e-safety incidents within this policy, the school's Designated Safeguarding Lead will contact the appropriate authorities, including Social Services and the police, if necessary and appropriate the DSL will also contact parents /guardians concerning incidents of inappropriate behaviour or relationships in school, and where know, to inform parents about incidents that occur out of school, but which effect members of the student body.

The **Headteacher** is responsible for:

Ensuring the safety of members of the school community, but day to day responsibility is delegated to the SDL and with reference to the designated school governor/s who have received Safeguarding training. There is a responsibility on all staff, including teaching assistants and learning support teachers to be aware of and uphold the aims and practice of this policy.

The **Headteacher and DSL in partnership with the ICT Teacher** are also responsible for:

- making arrangements for ongoing training
- make sure there are systems in place for monitoring the implementation of this policy and the mitigation of risk.
- To record all incidents and near misses in the Safeguarding log and to take appropriate action.
- The governor with training for safeguarding and e-safety incidents as they occur and these should be part of the Head teacher's report presented at every full

governors meeting (every 2 months).

Staff responsibilities:

- to be aware of the policy and to ensure that it is implemented on a day to day basis as part of their general teaching responsibilities.
- to be vigilant in matters of e-safety.
- Give regard to issues of internet safety in the research and planning of their lessons.
- To be aware of the schools acceptable use of e-safety expectations and to comply with them.
- Report any suspected misuse or problem or near miss to the SDL.
- The ICT teacher should ensure that safety training is embedded in the formal ICT curriculum.

Students responsibilities:

- Use the school's ICT systems with the student acceptable use agreement which they must sign at the beginning of each school year.
- Develop good practice and sound judgement in using technology in and out of school.
- Understand the importance of reporting abuse, misuse and inappropriate access to devices to staff.
- Follow school policies on mobile phones, devices, etc.

Means:

Risk and Dangers

	Commercial	Aggressive	Sexual	Values
Content The child as recipient	Advertisements Spam Sponsorship personal Information	Violent/hateful content lifestyle sites	Pornographic or unwelcome sexual content	Bias Racism Misleading advice or information
Contact The child as a participant	Tracking Grooming information	Being bullied, harassed or stalked	Meeting Strangers Being groomed	Self Harm Unwelcome persuasion
Conduct The child as participant	Illegal downloading Hacking Gambling Financial Scams Terrorism	Bullying or harassing an other person	Creating and uploading inappropriate materials Sexting	Providing misleading information and advice Health and well being: time spent on line

Digital imaging technologies and the internet in general have brought revolutionary and positive changes to teaching and learning. However staff and students must be aware of the risks associated with the indiscriminate posting and sharing of images and information on the internet and of misusing forms of e-communication.

The school will inform and educate students and other users about the risks involved and implement policies to reduce the potential for harm.

When using digital cameras or devices that can record images, staff will inform students about the risks associated with the, taking, sharing, publication and distribution of images. Especially they should recognise the risk attached to publishing images of themselves on, for example, facebook and other social networking sites.

Staff are permitted to take images of students only for educational purposes but must take care that students are appropriately dressed and are not taking part in activities that will bring the school into disrepute.

Staff must take pictures on school devices and these must be left in school in the locked cabinets provided. Photographs not required for historical purposes will be deleted at the end of each term and at other appropriate times. In accordance with our requirements of the Data Protection Act 1998, personal data will be recorded, processed, transferred and made available in legal ways, for limited and prescribed purposes, not excessive, accurate as far as you know, kept no longer than is necessary, secure and transferred to others with adequate protection.

In relation to photographs of students selected for publication, only those students whose parents have given permission will be used. Student's full names will not be used. Students work will not be published on the school website unless permission form student and parents/guardians has been given.

Support for safety and security:

The school will ensure that the ICT infrastructure and networks will be as secure as is reasonably possible. Specifically:

- Servers, wireless systems and cabling will be securely located and access restricted.
- Users will have defined access rights.
- All users from KS3 upwards will have a secure password for their work.
- The school will install and maintain a suitable filtering, monitoring security anti virus mechanism.
- The school will monitor and record user activity.

The school will establish the following good practice:

- Staff and students must use the bx.org.uk email platform to communicate on all

aspects of school work.

- Staff must monitor the appropriateness of their own communication and that of students and bring up inappropriate incidents of communication: staff and students
- must report any instance of email communication which makes them feel uncomfortable, is bullying or offensive in nature to the DSL.
- Students will be taught about email safety and the risks attached to the sharing personal details and personal images. Students will also be taught how to communicate appropriately via means of e-communication.

The following sets out the school rules for the use of communication technology in school:

For students the coverall rule can be summed up as 'devices use: educational recreational'.

	Staff				Students			
	Allowed	Allowed in lesson	Allowed with permission	Not Allowed	allowed	Allowed in lessons	Allowed with permission	Not Allowed
Mobile phones in school	√	√			√ after Y7		√	
Using mobiles in lessons	√	√					√	
Taking photos on personal mobiles or devices				√				√
Use of school hand held devices	√	√			√	√		
Use of school devices for taking photos including those of students			√*				√*	
Use of personal emails for school communication				√				√
Use of school email address for school based work, communication with peers or staff	√	√			√	√		
Use of school emails for group chat				√				√

Use of social networking sites			√*					√
Use of school email for personal emails				√				√
Use of twitter except for educational purposes				√				√
Befriending others on social networks on school devices				√				√

* For activities that are part of your responsibilities at the school. Photos taken of students must be for valid educational purposes.

Training, Learning and Teaching

Students

At the core of the above rules is **the training of the students to behave appropriately as a matter of their own personal choice.**

The school will therefore:

- Reinforce the regulatory framework such as age-limits applied, for example, to both social networking sites and gaming sites, and will inform parents when such regulations are breached.
- A planned e-safety teaching and learning programme will be provided as part of the ICT curriculum and will be age appropriate and form part of the signing of the agreement partnership signed at the beginning of each school year.
- Key e-safety themes and messages will be reinforced in all lessons where ICT is used and in form times and special assemblies and students will be taught the skills necessary to develop critical evaluation in students regarding materials they can access on line
- Rules governing the use of ICT in the school will be displayed in all teaching rooms

Parents

'There is a general divide,' (Byron Report) 'Many parents have only a limited understanding of e-safety risks, even though they play an essential part in, educating, regulating and monitoring their children's on line experience. Many will underestimate the potential for their children to access potentially harmful and inappropriate material. They are often similarly unsure of what to do when it happens.

The school will therefore seek to provide information for parents and arrange events to raise awareness and improve knowledge through.

- Newsletters

- the school website
- Parents evenings
- refer parents to helpful websites
- annual training events for parents
- parents may be told that their children's access to school systems and devices will be conditional of their children's ability to adhere to the schools agreed usage policy.

5

Staff

- annual training and review of the policy as part of the INSET training at the start of each academic year.
- New staff will receive guidance as part of their induction to the school.
- Volunteers will receive guidance as part of their induction to the school.
- The DSL should receive relevant training on issues of e-safety.

Curriculum

- in lesson, where internet use is preplanned, students should be guided to sites which have been checked as suitable.
- Students should be encouraged to alert staff if they come across an unsuitable material whilst using the schools devices.
- Staff should be vigilant in monitoring students if they are using the internet freely to search for material.
- Students should be taught to critically evaluate the material they access on the internet.
- Older students should be taught to acknowledge and reference the source of material in essays or coursework.

Reviewing this policy

- Day to day responsibility for implementing and upholding this policy lies with the teacher.
- It is the responsibility of students to report unacceptable material and unacceptable use of the internet or devices to staff.
- It is the responsibility of staff to report misuse of the internet to the DSL
- The DSL should inform the head and the designated safeguarding governor who will agree with the DSL of appropriate action to be taken on serious incidents. Details should also appear in the Head teacher's report.

Summary:

- e-safety will be monitored in school by the designated Safeguard Lead, who is also the 'go to' person for staff. Training should be annual for staff and part of the induction information passed onto new teachers and volunteers. Students and their parents must sign an annual agreement on safe internet use at the start of each school year. Students will receive education on e-safety as part of their curriculum, especially their ICT curriculum. Awareness will be kept at an appropriate level through various events throughout the school year.

This policy was written with due regard to the following documents and legislation:

The following school Policies

- Child Safeguarding
- Behaviour and Discipline
- Learning and Teaching or the Curriculum
- Anti-bullying
- Data Protection [Including the Data Protection Act of 1998]

- 'Safer Children in a Digital Age.' The Byron Report 2010

Date of review November 2015

Date of next review November 2017

Appendices:

1. Primary Students acceptable use agreement
2. Parent version of Primary Student Acceptable Use Agreement
3. Secondary Student Acceptable Use Agreement
4. Staff and Volunteer Acceptable Use Agreement
5. Proforma: e-safety Actions and Sanctions- Staff
6. Proforma: e-safety Actions and Sanctions- Students
7. Definitions of inappropriate activities

Appendix 1: PRIMARY STUDENT ACCEPTABLE USE AGREEMENT

I understand that I must use the school devices carefully and treat them with respect.

I understand that when I use the internet at school I must be careful to follow the school rules that are in this agreement.

For my own personal safety

- I understand that the school will be watching what I do online.
- I will be aware of 'stranger danger' when I am talking to people or characters online.
- I will not tell anyone my age, or where I live or when my birthday is or where I go to school.
- I will not arrange to meet people in real life.
- I will tell an adult straight away if I see or hear anything that makes me worried or scared.

I understand that everyone has equal rights to use the devices and

- I understand that the devices are meant for educational use and that I will not play on them unless I have permission to do so.
- I will not use the laptops for online games or YouTube unless I have permission to do so.
- I will not steal or damage the school laptops or any equipment, such as DS's, Ipods, phones or any other electronic device belonging to others.

I will act as I expect others to act toward me:

- I will respect others' work and the things that belong to them.
- I will not change their work or delete anything that belongs to them.
- I will be polite and responsible when I talk to others online. I will not use strong, aggressive or inappropriate language.
- I will not take pictures or send them to anyone else without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not bring a phone or any other device into school that can take photographs or video.
- I understand the risks and will not try to download or view any materials which are illegal or inappropriate or may cause harm or distress to others.
- I will immediately report any damage to the laptops or things that have gone wrong, however this may have happened.
- I will not click on any 'pop ups' or adverts I see.
- I will not use chat and social networking sites such as Club Penguin or Moshi Monsters when I am at school.

When using the internet for research or recreation, I recognize that:

- When I am using the internet to find information I should check that the information that I find is true. I understand that I cannot believe everything I read online.

I understand that I am responsible for my actions, both in and out of school:

- I understand that there will be consequences if I break this agreement when I am out of school and where it involves others belonging to the school. (examples would be cyber-bullying, use of images or personal information)
- I understand that if I break this agreement I will be disciplined.

Please sign your name below to show that you have:

1. read this agreement. 2. you understand the agreement 3. you agree to the rules

Your Name:

Year Group:

Date:

Appendix 2: PARENTAL VERSION OF THE PRIMARY STUDENT ACCEPTABLE USE AGREEMENT

New technologies have become integral to the lives of young people in today's society. The internet and other digital information and communications technologies are powerful tools and stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people are nonetheless entitled to be safe when making use of the internet.

This Acceptable Use Policy is intended to ensure:

- that young people 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 the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Primary Student Acceptable Use Agreement – Parent’s Version

- 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.

For my own personal safety:

- I understand that the school will monitor my use of the ICT systems, email and other digital communications.
- 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.
- I will not arrange to meet people off-line that I have communicated with on-line.
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

I understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- I will not use the school ICT systems for on-line gaming or watch videos unless I have permission of a member of staff to do so.
- I will not steal, disable or cause any damage to school equipment, or the equipment belonging to others.

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 the owner’s knowledge and permission.
- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will not bring a phone or any other device into school that can take photographs or video.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not click on any pop ups, or adverts or any links to other sites without permission from the teacher.
- 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 not use chat or social networking sites in school.

When using the internet for research or recreation, I recognise that:

- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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 (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

PRIMARY STUDENT ACCEPTABLE USE AGREEMENT FORM

**I have read and understand the above and agree to
following these guidelines when he/she is using school systems or doing work connected with school on other systems. I have read the Children's Version of this agreement with and have explained it to them.**

Name of parent:

Signed:

Date:

Appendix 3: SECONDARY STUDENT ACCEPTABLE USE AGREEMENT

New technologies have become integral to the lives of young people in today's society. The internet and other digital information and communications technologies are powerful tools and stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people 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 the security of the systems and users at risk.

The school will try to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users.

Student Acceptable Use 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.

For my own personal safety – in school:

- I understand that the school will monitor my use of the ICT systems, 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 immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.
- I understand that it is never too late to ask for help, regardless of what I have done.
- I know who can help me or where to go to get help if there are problems.

Additional personal safety – out of school:

- 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 understand that everyone has equal rights to use technology as a resource and:

- I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.
- 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 not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.
- I will not steal, disable or cause any damage to school equipment, or the equipment belonging to others.

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 the owner's knowledge and permission.

- I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

I recognise that the school has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the school:

- I will only use my personal held/external devices (mobile phones / USB devices etc) in school 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 immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- 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 only use chat and social networking sites with permission and at the times that are allowed.

When using the internet for research or recreation, I recognise that:

- I should ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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 (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to school ICT systems.

STUDENT AGREEMENT

I have read and understand the above and agree to follow these guidelines when I am using school systems or doing work connected with school on other systems.

Name of student:

Year Group

Signed:

Date:

Parent counter signature:

Date:

Please print name:

Appendix 4: STAFF AND VOLUNTEER ACCEPTABLE USE AGREEMENT

School Policy

New technologies have become integral to the lives of young people in today's society. The internet and other digital information and communications technologies are powerful tools, which 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 the security of the systems and user at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

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

Acceptable Use 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 students 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.

For my professional and personal safety:

- I understand that the school will monitor my use of the school 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, VLE etc) 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 not disclose my username or password to anyone else, nor will I try to use any other person's username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident, I

become aware of, to the appropriate person.

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 and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with appropriate permissions 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. Where these images are published (eg on the school website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in school in accordance with the school's policies.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

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

- When I use my personal hand held/external devices (PDAs/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 ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- I understand that my data is regularly backed up, in accordance with relevant school policies, e.g. Data Protection.
- 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 will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Data Protection Policy. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student 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.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not take photos of students on my own devices and will only take photos on school devices for valid educational reasons.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

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 5: e-Safety: Log of Actions and Sanctions – Staff

Name of member of staff:	Refer to ICT coordinator for advice	Verbal warning	Refer to SLT	Written warning	Disciplinary action
Brief details of incident					
DELIBERATELY ACCESSING OR TRYING TO ACCESS MATERIAL THAT COULD BE CONSIDERED ILLEGAL					
Excessive or inappropriate personal use of the internet / social networking sites / personal email					
Using personal email, social networking, instant messaging and text messaging to communicate with students					
Unauthorised downloading or uploading of files					
Accessing or allowing others to access school network by sharing usernames or passwords					
Accessing or attempting to access the school network using another person's username or password					
Careless use of personal data e.g. holding or transferring data in an insecure manner					
Deliberate action to breach data protection, copyright, licensing regulations or network security					
Corrupting or destroying the data of others or causing deliberate damage to hardware or software					
Sending a message that causes offence or could be regarded as harassment or bullying					
Actions which breach the					

integrity of the values and ethos of the school					
Actions which compromise the staff member's professional standing					
Taking photos of students on personal devices or taking photos for reasons other than of valid educational use.					
Using proxy sites or other means to subvert filtering systems					
Accidentally accessing offensive or pornographic materials and failing to report the incident					
Deliberately accessing or trying to access offensive or pornographic material					
Continued infringements following previous warnings or sanctions					

Brief details:

Date:

Written by:

Appendix 6: e-Safety: Log of Actions and Sanctions – Students

Name of student:	Warning by teacher	Inform SLT	Inform parents	Refer to the police	Removal of right to use school devices	Suspension	expulsion
DELIBERATELY ACCESSING OR TRYING TO ACCESS MATERIAL THAT COULD BE CONSIDERED ILLEGAL							
Unauthorised use of non-education sites during lessons							
Unauthorised use of mobile phone, camera or other hand-held device							
Unauthorised use of social networking / instant messaging / personal email							
Unauthorised downloading or uploading of files							
Accessing or allowing others to access school network by sharing usernames or passwords							
Accessing or attempting to access the school network using another person's username or password							
Corrupting or destroying the data of others							
Sending a message that causes offence or could be regarded as harassment or bullying							
Continued infringements following previous							

warnings or sanctions							
Actions which breach the integrity of the values and ethos of the school							
Using proxy sites or other means to subvert filtering systems							
Accidentally accessing offensive or pornographic materials and failing to report the incident							
Deliberately accessing or trying to access offensive or pornographic material							
Receipt or transmission of copyright material or breaches of Data Protection Act							
Taking photos of other students on own or school devices without others permission of for purposes other than valid educational reasons.							

Brief description of incident:

Date

Location:

Action:

Written by:

Appendix 7: Definitions of Inappropriate Activities

Child sexual abuse images
Promotion or conduct of illegal acts under, e.g., child protection, obscenity, computer misuse and fraud legislation
Adult material that potentially breaches the Obscene Publications Act in UK
Criminally racist material
Pornography
Promotion of any kind of discrimination
Promotion of religious or racial hatred
Threatening behaviour, including the promotion of physical violence or mental harm – ‘cyber-bullying’
Any information offensive to other persons or that breaches the integrity of the ethos and values of the school
Using school based systems to run a private business
Use systems, applications, websites, etc., that bypass the filtering or other safeguards used by the school
Up/downloading or transmitting commercial software or copyright materials without licence or consent
Revealing or publicising confidential or proprietary information
Creating or propagating computer viruses or other harmful files
Sustained/instantaneous high volume network traffic so as to cause network congestion thus hindering others
On-line gaming (educational)
On-line gaming (non-educational)
On-line gambling
On-line shopping or other commercial activity
File sharing
Use of social networking sites
Use of video broadcasting, e.g. downloading Youtube
Use of video broadcasting e.g. uploading
Taking Photos of other students for non educationally valid purposes and using them for

any purposes whatsoever.