E-Safety Policy

Approved by Governors on 19 November 2015

Signed

Review: Autumn Term 2017

E-SAFETY POLICY

Mission Statement

"*Love one another as I have loved" (John, 15)*

We believe that Jesus Christ and his Gospel Call – to love God and all people – are at the heart of what we do.
He inspires us, as children of God, to uphold the dignity of each individual.
We strive to develop a community in Christ which fully supports all in achieving their potential – spiritually, academically and personally.

Contents

E-Safety Policy

Rationale

Christ the King uses many different types of ICT equipment for educational purposes. This document outlines guidelines on the use of this equipment for staff, students and parents/carers. Please read this document carefully and return the last page signed to the main office.

This policy applies to all members of the school community (including staff, students, parents/carers, visitors and school community users).

Research has proven that use of technology brings enormous benefits to teaching and learning. However, as with many developments in the modern age, it also brings an element of risk. Whilst it is unrealistic to eliminate all risks associated with technology, the implementation of an effective E-Safety Policy will help children to develop the skills and confidence to manage potential risks and considerably reduce their impact.

Our E-Safety Policy, as part of the wider safeguarding agenda, outlines how we will ensure our school community are prepared to deal with the safety challenges that the use of technology brings. The policy is organised in 4 main sections:

Policies and Practices

Infrastructure and Technology

Education and Training

Standards and Inspection.

Introduction
The role of Staff, Student and Parents in relation to E-Safety

Designated E-Safety Officer: Mr Clarke (Head of ICT)

ICT Teachers

To deliver E-Safety content at the start of each academic year to all year groups, with a review during E-Safety Week and Internet Safer Day. To also ensure that all other staff are trained and are aware of how to report incidents following correct procedures and requirements should an incident occur with the assistance of the Network Manager.

Network Manager

To manage and monitor network devices such as computers and laptops, to ensure that relevant security procedures are adhered to, keeping up to date with emerging technologies.

Teaching and Support Staff

To promote good E-Safety practice in their lessons when it is relevant and appropriate.

Student Representatives

To offer advice to the persons responsible for E-Safety on the current and latest technology they feel may be an E-Safety issue, also promoting good E-Safety etiquette to other peers.

Other Students

To respect and promote E-Safety to other peers when in school and in the wider community.

Parents

Parents and carers have a responsibility for discussing E-Safety with children and for backing up the E-Safety measures that children have learned at school by reinforcing them at home.

Parents should be encouraged to talk to their children about what they do online. Children and parents should use technology together where relevant, learning and having fun.

By having open and ongoing conversations with children about technology, parents will also have more opportunity to talk to children about being safe and responsible online. Children are also likely to feel more comfortable about discussing any problems or concerns that they have.

Section 1:
Policies and Practices

This E-Safety Policy should be read in conjunction with the following related policies and documents:

Student: Internet and Email Acceptable Use Policy

Staff: ICT Security Framework Policy (this contains the staff AUP)

Think Before You Click

Christ the King encourages a "Think before You Click" ethos. Students and staff should ask themselves three questions before they click:

- Is the information likely to be accurate?
- Can I be sure online people or friends are who they say they are?
- Would I do this if my parents/carers or another person was with me?

Think Before You Type

Christ the King employs a "Think before You Type" Ethos. Students and staff should ask themselves three questions before they type:

- Would I want this information to be directed at me?
- Can I be sure that I will not face repercussions for this statement?
- Would I do this if my parents/carers or another person was with me?

1.1 Security and Data Management

In line with the requirements of the Data Protection Act (1998), sensitive or personal data is recorded, processed, transferred and made available for access in school. This data must be:

- Accurate
- Secure
- Fairly and lawfully processed
- Processed for limited purposes
- Processed in accordance with the rights of the individual
- Adequate, relevant and not excessive
- Kept no longer than necessary
- Only transferred to others with adequate protection.

For further information with regards to security of data please refer to the ICT Security Framework Policy.

Internet

All staff and students have access to the internet for the purpose of teaching and learning. All internet traffic is filtered to protect staff and students from inappropriate material; however no filtering solution is 100% successful. Any inappropriate material should be reported to a member of staff. At Christ the King we manage our own filtering in house, this allows us greater flexibility to what staff and students can view giving the students a greater awareness of what content is actually available on the internet, this is known as a managed system.

Staff and Students should not search for inappropriate content; use bad language or access chat rooms/forums unless directed by a member of staff.

The school reserves the right to monitor and examine any internet sites visited by students or staff.

The school states that:

- The school will maintain a current record of all staff and students who are granted access to the school's electronic communications.
- All staff will read and sign the 'ICT Security Policy" before using any school ICT resources.
- Parents and students will be asked to read the School Acceptable Use Policy for student access and discuss it, where appropriate.
- All visitors to the school site who require access to the schools network or internet access will be asked to read and sign the ICT Security Policy.

The school will take all reasonable precautions to ensure that users access only appropriate material. However, due to the global and connected nature of Internet content, it is not possible to guarantee that access to unsuitable material will never occur via a school computer. Neither the school nor Lancashire County Council can accept liability for the material accessed, or any consequences resulting from Internet use.

1.2 Use of mobile/handheld devices

Hand held devices that are brought into school such as smart phones can be used to access the unfiltered internet therefore cannot be monitored. As a result of this personal mobile devices (phones, cameras, mp3 players, game consoles) are not allowed in school. However, e-readers with pre-downloaded content are allowed with prior permission and signed parental consent regarding liability. If a student uses a mobile device on the school premises the device will be removed and will only be returned to a parent/carer or to another responsible adult. If the device has been used to record or store images of students/staff without their consent, the school reserves the right to remove all of the material before it is returned.

Any handheld devices used to access the data on the school system such as download emails to smartphones is allowed provided the phone has relevant security measures in place such as encryption to prevent a breach in data protection should these devices be lost or stolen. Staff should not store any types of media related to students on their personal devices. Students should ask

permission if they wish to use their own personal device. The school is not liable to support any of these devices if they don't work with the system.

Student Use of Personal Devices

- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents/carers in accordance with the school policy.
- Phones and devices must not be taken into examinations. Students found in possession of a mobile phone during an exam will be reported to the appropriate examining body. This may result in the student's withdrawal from either that examination or all examinations.
- If a student needs to contact his/her parents/carers they will be allowed to use a school phone. Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences.

Any laptops issued to students are the responsibility of the student and the parents/carers where the parent should enforce the E-Safety Policy taught at school. Students and parents will have been notified about the correct policy and procedures at the time of issue of the laptop.

Removable Media

Removable media such as USB pens and portable hard disk drives are allowed to be used with the schools computers. However students have a responsibility to make sure these items are virus free and only contain content that is school work related. The school reserves the right to examine any removable media that is brought into the school. Should staff store confidential information on removable media these devices should be encrypted.

Staff and students should report any virus warnings to a member of staff. If a virus is detected on any removable media the Network Support Team will examine the device and offer the best advice possible at the time.

If any material on a removable media device is deemed to be inappropriate action may be taken by the students' Achievement Co-ordinator or the E-Safety Officer.

1.3 Use of Digital Media

Various forms of digital media offer substantial benefits to education but equally present schools with challenges particularly regarding posting or sharing media on the Internet, through mobile technologies and Social Network sites.

In our school we are aware of the issues surrounding the use of digital media online. All members of our school understand these issues and need to follow the school's guidance. As photographs and videos of students and staff are regarded as personal data in terms of The Data Protection Act (1998), we must have written permission for their use from the individual and/or their parents or carers. For further information please refer to the main office that holds consent for each student.

Staff and students at Christ the King are educated about the risks surrounding taking, using, sharing and publishing and distributing digital media.

Some of the risks that can arise from publishing digital media are:

- Embarrassment
- Invasion of privacy

Some key points to remember are:

- Has the person given me consent to use this digital media?
- Would I want this digital media to be published about myself where everyone can see it?
- Is this digital media invading someone's privacy?

Should digital media of students and staff be used for official publications consent should have been obtained prior to the use of the digital media, at no time will a name of the student or staff be used with the digital media.

Visitors

When parents/carers and visitors attend a school event they should be made aware of this policy and should seek permission before obtaining any digital media such as photographs.

Personal Devices

For staff and students it is unacceptable to store any digital media on any personal devices, should they wish to make use of digital media the ICT Department have a range of cameras and video recorders for such occasions.

1.4 Communication Technologies

As a community we use a variety of communication technologies for school and personal purposes such as email, social networking and texting.

Email:

Email is used by all staff and students, the only email system that should be used for communication to do with Christ the King should be the email account provided by the school. Should parents wish to contact the school via email they should direct their emails to reception@ctk.lancs.sch.uk, who will then pass this on to the relevant member of staff as soon as possible. Staff and students should not use personal email accounts during school hours or for professional purposes.

Each individual is responsible for the emails that are sent from their email account. All emails sent should be appropriate and be in polite manner. Students should not use emails to communicate with bodies or persons outside of Christ the King unless a member of staff has given permission to do so, as you are representing the school.

Any email sent using this account should not contain any bad language, negative references about other students/staff/the school or any material that can be deemed as threatening or inappropriate. Should students receive any email of this nature this should be reported to the appropriate member of staff.

The school reserves the right to monitor, examine and delete any emails sent using the school email system.

As emails enter and leave the school network they are all scanned for SPAM/ Viruses, however please be vigilant when opening emails from unknown sources, should you be in doubt please seek advice from the ICT Support Team.

E-mail Good Practice – this can also be found in the ICT Security Policy.
The following guidelines (some of which also apply to other forms of correspondence) tell you what is and what is not good practice when you use the Internet and email services.

Students & staff should:

- Check your email inbox for new messages regularly;
- Only use the school email system for official school business or school social events;
- Treat email as you would a letter, remember they can be forwarded / copied to others;
- Check the email message and think how the person may react to it before you send it;
- Make sure you use correct and up to date email addresses;
- File email when you have dealt with it and delete any items that you do not need to keep;
- Only email the recipient you wish to communicate with;
- Only use the approved, secure email system(s) for any school business.

You should not:

- Use email to message staff where face-to-face discussion is more appropriate;
- Create wide-distribution emails (for example, all staff) unless this form of communication is vital;
- Print out email messages you receive unless you need a hard copy;
- Insert and send large file attachments to emails to many addressees;
- Send an email that the person who receives it may think is a waste of resources;
- Use jargon, abbreviations or symbols if the person who receives the email may not understand them;
- Open any attachments or links if you don't know the person who has sent them;
- Use email as a public forum to express opinions or concerns;
- Click on any Internet advertisement banners.

Social Networks:
Social networking sites can connect people with similar or even very different interests. Users can be invited to view personal spaces and leave comments, over which there may be limited control. For responsible adults and young people, social networking sites provide easy to use, free facilities, although advertising often intrudes and some sites may be dubious in content. Our students are encouraged to think about the ease of uploading personal information, the associated dangers and the difficulty of removing an inappropriate image or information once published.

Parents are advised the legal minimum age for the use of social networking sites is 13.

Social networking sites are blocked for all staff and students in school.. However, comments made outside of school on these sites may contravene confidentiality or bring the school, staff or students reputation into disrepute therefore students and staff are encouraged to think before posting anything online.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Social Network sites for both staff and students:

You should:

- “Think before you type”
- Only accept people you know as friends
- Report anything that you feel uncomfortable with (online reporting tools such as Child Exploitation and Online Protection (CEOP)
- Be aware of the online dangers of social networking frape
- Set your profile to 'Private so only your friends can see it
- Only post something you want your parents, teachers, the police or even future employers to read.
- Consider not posting photos of yourself. They can be altered and used in upsetting ways.
- Be cautious about posting details that could be used to locate you: e.g. the name of your school, sports team or where you work.
- Check the sites' safety policies. Find out how to report violations and how to get them removed.
- Show your parents your profile - even if you don't add them as friends!

You should not:

- “Frape” anyone (The act of using someone else’s online profile/account to post information on their behalf without their consent)
- Post images of other members of the school without obtaining prior consent
- Set up a group related to Christ the King without our prior consent from the Headteacher
- Post comments about anything to do with the school

- Post personal information
- Disclose your location on social networking sites
- Staff will not communicate with students using social networking
- Students will not communicate with staff using social networking
- Post personal identifiers like your address, phone number, age or date of birth.
- Forget that once you post online, you can't take it back. Deleted posts and profiles don't always stay deleted.
- Assume that people are who they say they are. One in five Facebook profiles are fake.
- Arrange to meet new online friends in real life. If you do, meet in a public place and go with a friend. Tell your parents where you are going.
- Be a phishing victim. Never open files you didn't ask for or expect and if you see suspicious links or prompts asking you to log in again - don't click them.
- Join new social networks without checking their privacy policies - some sites share your information (like your email address) with companies who send you spam.

Staff understand that they must not make 'friends' or interact online with current or former pupils under the age of 18 using any social networking sites. This includes gaming on the internet using websites, apps or game consoles. Staff also understand that the school recommends that staff using social networking sites restrict contact with parents and carers of current and former pupils to those with whom they have a personal friendship.

Web sites / Virtual Learning Environment (VLE) and other online publications:
At Christ the King we have a school website which acts as a communication tool delivering key and up to date information to members of the wider community. The content on the website must be approved by SLT before publication. We also have a VLE to assist our students with their learning, allowing students to access online resources that have been developed by our members of staff or students.

In our school the following statements outline what we consider to be acceptable and unacceptable use of Websites and other online publications:

Acceptable

- Content is professional
- Content is spell checked / Proof Read
- Content is approved by the relevant member of staff

Unacceptable

- Bad Language
- Inappropriate Images
- Out of Date content

- Abuse of forums

Other

Currently there are online storage methods that allow users to share any resources for free such as Drop Box, Google Drive, One Drive. Students are not to access any personal online storage methods unless agreed with an appropriate member of staff, should the student be granted permission the student accepts there is no in appropriate content contained in this online storage. Staff will not use online storage facilities to share school information containing personal details.

In our school the following statements outline what we consider to be acceptable and unacceptable use of the above:

Acceptable

- Ask permission before use
- Share legal academic resources

Unacceptable

- Accessing these methods without permission
- Online storage facilities contain inappropriate information
- Storing Personal details relating to the school and our students

As a school we do not support online storage methods provided by third parties, we accept no responsibility for anyone using these methods.

1.5 Acceptable Use Policy (AUP)

Christ the King currently have a number of Acceptable Use Policies (AUPs) in place to ensure that all users stay safe whilst using the internet and other communication technologies. Please refer to the appropriate policy for further guidance which works alongside the E-Safety Policy.

Student: Internet and Email Acceptable Use Policy

1.6 Dealing with incidents

All E-Safety incidents must be recorded by the designated E-Safety Officer. This incident log will be monitored and reviewed regularly by the Headteacher, Governors and the ICT Development Group.

Section 2:
Infrastructure and technology

Christ the King is responsible for ensuring that the network infrastructure is as safe and secure as possible. This section of the policy defines the policies and procedures in place to safeguard users.

Student Access:

Students are only to access computers when there is a member of staff present and they have asked permission before hand. At no times should the students be left un-attended when using the computer systems. All students are given a unique user name and password.

Students that started before 2012 their username follows the following format:

First initial, Surname eg Joe Blogs would be jblogs

Students that started on or after 2012 their username follows the following format:

Year they started Surname, First Initial eg Joe Blogs started in 2012 would be 12BlogsJ

Students should keep their logon details safe and should not share this information with anyone, and are advised to change their password regularly. Students are held responsible for their own logon account. Christ the King reserves the right to access any account provided by us, without prior consent.

Managing the Network and Technical Support:

The ICT Support Team is responsible for technical support in school and will provide the appropriate level of access required.

- All network equipment is secured in locked rooms and cabinets.
- All computers are regularly updated, patched and are closely monitored.
- Anti-virus runs on all computers, the anti-virus that is currently used is Sophos which is provided by the local authority.
- Students are required to log off the computers at the end of each lesson, they can lock them during the lesson.
- Staff are required to lock their computers when they are not in use.
- Students are not permitted to install any software or possess any inappropriate file types such as: .exe, .bat
- Staff should ask permission before they install any software. This will be down to the discretion of the Network Manager whether it should be installed.
- All computer systems are monitored for staff and students.

Section 3:
Education and Training

Responsibility of E-Safety Officer and S Newton

Working and Educated offsite

Staff and students are reminded to follow this E-Safety Policy when they are working away from Christ the King. Please note that additional E-Safety policies may also have to be followed in the new environment depending on the educational establishment or work placement.

3.1 E-Safety across the curriculum

Responsibility of E-Safety Officer

We believe that the key to developing safe and responsible behaviours online, not only for students but everyone

- Within our community, lies in effective education. We know that the Internet and other technologies are embedded in our students' lives not just in school but outside as well, and we believe we have a duty to help prepare our students to safely benefit from the opportunities the Internet brings.
- We will provide a series of specific E-Safety-related lessons in every year group as part of the ICT curriculum.
- We will celebrate and promote E-Safety through a planned programme of assemblies and whole-school activities, including promoting Safer Internet Day each year.
- We will discuss, remind or raise relevant E-Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use, and the need to respect and acknowledge ownership of digital materials.
- School will ensure that the use of Internet derived materials by students and staff complies with copyright law
- Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy
- We will remind pupils about their responsibilities through an end-user Acceptable Usage Policy which will be displayed throughout the school and have to be accepted each time a pupil logs on.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

Training

Tips of day / week / month

Policy to be signed annually

E-Safety to be delivered during the staff induction program

Staff updated regarding any changes to the policy

3.2 E-Safety – Raising parents/carers awareness

Parents are asked to:

- Help and support the school in promoting E-Safety.
- Read, understand and promote the school pupil Acceptable Usage Policy with their children.

- Take responsibility for learning about the benefits and risks of using the Internet and other technologies that their children use in school and at home.
- Take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- Discuss E-Safety concerns with their children, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology.
- Model safe and responsible behaviours in their own use of technology.
- Consult with the school if they have any concerns about their children's use of technology.

We believe it is important to help all our parents develop sufficient knowledge, skills and understanding to be able to help keep themselves and their children safe.

To achieve this we will:

- Include E-Safety as part of the events on Consultation Days
- Include useful links and advice on E-Safety on our school website
- Provide parents with useful information from the ThinkUKnow and ChildNet websites
- Include a section on E-Safety in the School Welcome Pack and Home-School Agreement

Training

Flyers

Items on newsletters

Info on school website

3.3 E-Safety – Raising Governors' awareness

Governors are asked to:

- Read, understand, contribute to and help promote the school's E-Safety policies and guidance.
- Develop an overview of the benefits and risks of the Internet and common technologies used by students.
- Develop an overview of how the school ICT infrastructure provides safe access to the Internet.
- Develop an overview of how the school encourages students to adopt safe and responsible behaviours in their use of technology in and out of school.
- Support the work of the ICT Development Group in promoting and ensuring safe and responsible use of technology in and out of school, including encouraging parents to become engaged in E-Safety activities.
- Ensure appropriate funding and resources are available for the school to implement their E-Safety strategy.
- Educate all users on appropriate and responsible use of cloud storage in compliance with the 8 points of the Data Protection Act. Please refer to the Staff ICT Security Policy for more information.

Section 4:

Standards and Inspection

Responsibility of E-Safety Officer

Frequent reviews of incidents –

Examples of possible E-Safety incidents involving staff:

- Transferring personal data insecurely
- Using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- Failure to abide by copyright of licensing agreement
- Failure to follow guidelines set out in the Data Management and Security Policy.
- Where a member of staff is made aware of a possible E-Safety incident, they should inform the E-Safety Officer or Child Protection Officer who will then use the schools agreed procedure to respond in the most appropriate manner.
- Whilst resolving an incident those students involved may have their computer accounts suspended.

APPENDIX

Staff E-Safety Policy

Staff Use of Personal Devices

- Staff are not permitted to use their own personal phones or devices for contacting students and their families within or outside of the setting in a professional capacity, except with the permission of the Headteacher.
- Mobile Phone and devices will be switched off or switched to 'silent' mode, Bluetooth Communication should be "hidden" or switched off and mobile phones or devices will not be used during teaching periods unless permission has been given by a member of Senior Leadership Team in emergency circumstances.
- If members of staff have an educational reason to allow children to use mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team.
- Staff should not use personal devices such as mobile phones or cameras to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Laptops

All staff laptops that are taken off site are encrypted. Should a member of staff want to take a device home they should seek written permission from the Network Manager. All members of staff take full responsibility for the laptop once it has been loaned to them; please refer to the staff laptop agreement.

- Staff are required to lock their computers when they are not in use.
- Staff should ask permission before they install any software. This will be down to the discretion of the network manager whether it should be installed.

Social Networks:
Staff are reminded to recognise the need to behave in a professional manner at all times when using any form of communication technologies. If content is made available online it is available for everyone to see and remains there forever.

Acceptable Use Policy (AUP)

Christ the King currently have a number of Acceptable Use Policies (AUPs) in place to ensure that all users stay safe whilst using the internet and other communication technologies. Please refer to the appropriate policy for further guidance which works alongside the E-Safety Policy.

Staff: ICT Security Framework Policy (this contains the staff AUP)

Infrastructure and technology

Staff Access:

Staff that are required to access the computer system will be provided with all appropriate logon on details when they first join Christ the King. Before any access is granted staff will also be required to sign the ICT Security Framework Policy.

Staff are to accept full responsibility for their logon details, including emails. Staff are not to let students or other staff use their computer account at any time. Staff are advised to change their password regularly and keep it complex.

Christ the King reserves the right to access and monitor any staff account provided by us, without prior consent.

E-Safety – Raising staff awareness

- Read, understand and help promote the school's E-Safety policies and guidance.
- Read, understand and adhere to the school Staff Acceptable Usage Policy.
- Develop and maintain an awareness of current E-Safety issues and guidance.
- Model safe and responsible behaviours in their own use of technology.
- Embed E-Safety messages in learning activities where appropriate.
- Supervise students carefully when engaged in learning activities involving technology.
- Be aware of what to do if an E-Safety incident occurs.
- Maintain a professional level of conduct in their personal use of technology at all times.
- We will remind pupils about their responsibilities through an end-user Acceptable Usage Policy which will be displayed throughout the school and have to be accepted each time a student logs on.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

Standards and Inspection

Responsibility of E-Safety Officer

Frequent reviews of incidents –

Examples of possible E-Safety incidents involving staff:

- Transferring personal data insecurely
- Using digital communications to communicate with students in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or communicating via social networking sites)
- Failure to abide by copyright of licensing agreement
- Failure to follow guidelines set out in the Data Management and Security Policy.
- Where a member of staff is made aware of a possible E-Safety incident, they should inform the E-Safety Officer or Child Protection Officer who will then use the schools agreed procedure to respond in the most appropriate manner.
- Whilst resolving an incident those students involved may have their computer accounts suspended.

E-Safety Policy for Staff

I have read and understand the E-Safety Policy for Christ the King Catholic High School.

I accept and agree to abide by all the guidelines and policies set out in this framework.

Please print, sign and date below and then return this page to the Network Manager.

Staff Member (Print Name):	
Signed:	Date:

Acceptable Use of the Internet and E-mail

Christ the King has installed computers* and Internet access to help our learning.

These rules will keep everyone safe and help us be fair to others.

- I will only access the system with my own login and password, which I will keep secret
- I will not access other people's files
- I will only use the computers for school work and homework
- I will not bring in removable media from outside school, unless I have been given permission from a member of staff
- I will only e-mail in lesson time when given permission to do so
- The messages I will send will be polite and responsible
- I will always be myself and not pretend to be anyone or anything I am not
- I will not give my home address, my telephone number, my school name or arrange to meet someone, unless my parent, carer or teacher has specifically given permission
- I will not use lesson time to set up or access private e-mail accounts
- I will never respond to nasty, suggestive or rude e-mails or postings in online Groups
- I will report any unpleasant material or messages sent to me. I understand my report would be confidential and would help protect other students and myself
- I will never send anyone credit or bank details
- I will always remember if someone "makes me an offer which seems too good to be true," then it probably is
- I will respect copyright laws and will not download or copy materials without permission
- I will ask permission before opening an email or an email attachment sent by someone I do not know
- I will not use Internet chat
- I understand that if I deliberately break these rules, I will be punished accordingly
- I will not store inappropriate files in cloud storage or in my Documents and only use school approved cloud storage.
- I will not post any type of media of others onto social media
- I will make sure I have logged out of any cloud storage
- I will adhere to the E-Safety Policy at all times
- I will report any damages to hardware to my teacher right away
- I will not stream videos from the Internet unless I have permission
- I will use handheld technology appropriately at all times
- I will not create and use any personal hotspots in school

The school may exercise its right by electronic means to monitor the use of the school's computer systems, including the monitoring of web-sites, the interception of E-mails and the deletion of inappropriate materials in circumstances where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be being used for criminal purposes or for storing text or imagery which is unauthorised or unlawful.

*Computers include handheld devices

Student's Agreement

I have read and understand the school's "Acceptable use of the Internet and E-mail policy". I will use the computer system and Internet in a responsible way and obey these at all times.

Student's Name ……. BLOCK CAPITALS

Student's Signature: ……. Date: …….

Parent/Carer's consent for Internet Access

I have read and understood the school's "Acceptable use of the Internet and E-mail policy" and give permission for my son/daughter to access the Internet. I understand that the school will take all reasonable precautions to ensure students cannot access inappropriate materials. I understand that the school cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the school is not liable for any damages arising from use of the Internet facilities.

Parent/Carer's Name ……. BLOCK CAPITALS

Parent/Carer's Signature: …….. Date: …….