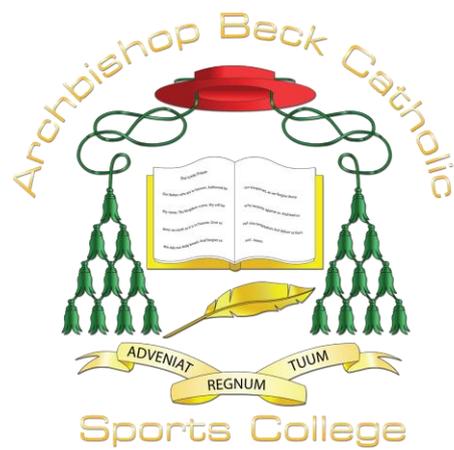


ARCHBISHOP BECK CATHOLIC SPORTS COLLEGE

E-SAFETY POLICY



Ratified: May 2014

Ratified by: Governors Staffing Committee

Review: May 2017



1. Development/Monitoring/Review of this Policy

This e-Safety policy has been developed by a working group made up of:

- College E-Safety Coordinator
- Headteacher / Senior Leaders
- Teachers
- Support Staff
- ICT Technical staff
- Governors

Consultation with the whole college community has taken place through the following

- Staff meetings
- Governors meeting / sub-committee meeting
- College website / newsletters

This E-safety policy was approved by the Governing Body/Governors Sub Committee on:	
The implementation of this e-safety policy will be monitored by:	The ICT Steering Group and the E-Safety Co-Ordinator
The E-Safety Policy will be reviewed at appropriate intervals or every three years, in the light of any significant new developments in the use of the technologies, new threats to e-safety or incidents that have taken place. The next anticipated review date will be:	The ICT Steering Group and the E-Safety Co-Ordinator

2. Scope of the Policy

This policy applies to all members of the college community (staff, students, volunteers, parents/carers, visitors and community users) who have access to and are users of the college ICT systems, both in and out of college.

The Education and Inspections Act 2006 empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other e-safety incidents covered by this policy, which may take place out of college, but is linked to membership of the college.

The college will deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents/carers of incidents of inappropriate e-safety behaviour that take place inside and outside of college.

3. Context

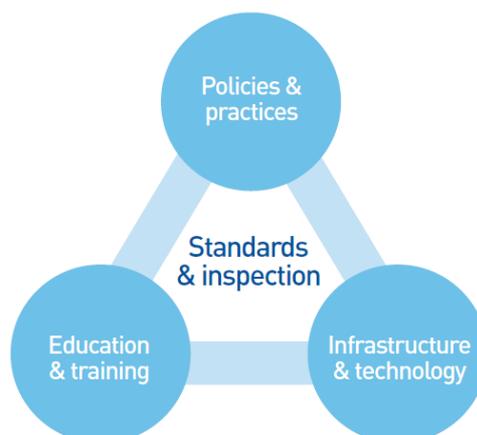
We live in a digital age where technology is playing an ever increasing part in our lives; it is changing the way that we do things both inside and outside of college and although we recognise the benefits of technology we must also be aware of the potential risks and ensure that all staff, students and parents/carers associated with the college are able to use technology in a safe and responsible manner.

Some of the potential dangers of using technology may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to/loss of/sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing/distribution of personal images without an individual's consent or knowledge
- Inappropriate communication/contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video/internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person.

Many of these risks reflect situations in the offline world but it is important that as a college we have a planned and coordinated approach to ensuring that all involved with the college use technology in a safe and responsible way. As with all risks it is impossible to eliminate them completely but with a planned and coordinated approach they can be significantly reduced and users can be taught to manage them effectively.

The college have adopted the PIES model which is the basis of it approach towards E-Safety and helps to manage and minimise its risk.



1) Policies and practices

The e-Safety policy outlines the importance of ICT within and outside of education. It provides guidance on the schools approach to E-Safety and details a code of conduct for school staff and students. The policy aims to provide an agreed, coordinated and consistent approach to E-safety. The code of conduct forms the basis of the colleges expected behaviours regarding the use of technology and any infringements of the code of conduct will lead to disciplinary action against the perpetrator(s).

2) Infrastructure and technology

The colleges access to the internet is provided by Liverpool City Council through its IT partner Liverpool Direct Limited (LDL). This network provides a safe and secure 10Mbps broadband connection to the internet via the LDL data centres. There is a multi-layer security shield that provides dual-layer firewall protection, intruder detection/prevention, load balancing, content caching, data traffic analysis and virus protection. There is a cloud-based filtering service, ScanSafe, which filters internet content using the City Councils base policy. ScanSafe undertakes live scanning of all sites and blocks any threats or inappropriate websites. The infrastructure has been designed to minimise the risk of; users accessing inappropriate material, data being lost or accessed by unauthorised users, virus or malware threats. All internet activity is logged via the LDL data centre and can be retrieved if required in the event of an investigation.

The college is responsible for ensuring that the college infrastructure/network is as safe and secure as is reasonably possible.

3) Education and training Standards and Inspection

As the use of technology and the potential risks associated with the use of the technology change rapidly, it is essential to ensure that the college community know how to use technology safely and responsibly. The college is committed to ensuring that staff receive regular training to keep up to date with new developments and ensure that they are sufficiently confident to educate students in the safe and responsible use of technology.

4) Standards and inspection

The college reviews its approach to E-safety on a regular basis and uses the 360° Safe tool to evaluate and improve its provision. Reference is also made to e-safety in the annual 175 audit and through Ofsted inspections.

4. Policy Statements

Whilst the PIES model forms the basis of the colleges approach to E-safety the college will ensure that all access to the internet and ICT systems by students is effectively managed and supervised.

As part of the E-safety policy the college will also manage:

- The use of digital images and video
- Data protection
- Digital communications
- Unsuitable/inappropriate activities
- Incidents of misuse

The use of digital images and video

The development of digital imaging technologies has created significant benefits to learning, allowing college staff and students instant use of images they have recorded themselves or downloaded from the internet. College staff and students are made aware of the potential risks associated with storing, sharing and posting images on the internet and must follow the good practice detailed below.

- When using digital images, staff will inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they will recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Staff are permitted to take digital images and video to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college equipment; the personal equipment of staff should not be used for such purposes.
- Care will be taken when capturing digital images and video that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute.
- Students must not take, use, share, publish or distribute images of others without their permission.
- Images and videos published on the college website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.
- Student's work will only be published with the permission of the student and parents or carers.

Data Security and Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 which states that personal data must be:

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

All college staff will ensure that:

- Care is taken to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Personal data is used or processed on only secure password protected computers and other devices and that these devices are properly "logged-off" at the end of any session in which they are using personal data.
- Data is transferred securely using encryption and secure password protected devices and email solutions.
- Personal data must not be stored on any portable computer system, USB stick or any other removable media.

Digital Communication

Digital communication is an area that is developing rapidly with new and emerging technologies, devices are becoming more mobile and information sharing/communication is becoming more sophisticated.

When using communication technologies the college ensures the following good practice:

- The official college email service is regarded as safe and secure and is monitored. Staff and students should therefore use only the college email service to communicate with others when in college, on college business or on college systems.
- Users need to be aware that email communications may be monitored
- Users must immediately report the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any digital communication between staff, students or parents/carers (email, chat, VLE etc) must be professional in tone and content. These communications may only take place on official (monitored) college systems. Personal email addresses, text messaging or public chat/social networking programmes must not be used for these communications.
- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material.

- Personal information will not be posted on the college website and only official email addresses should be used to identify members of staff.

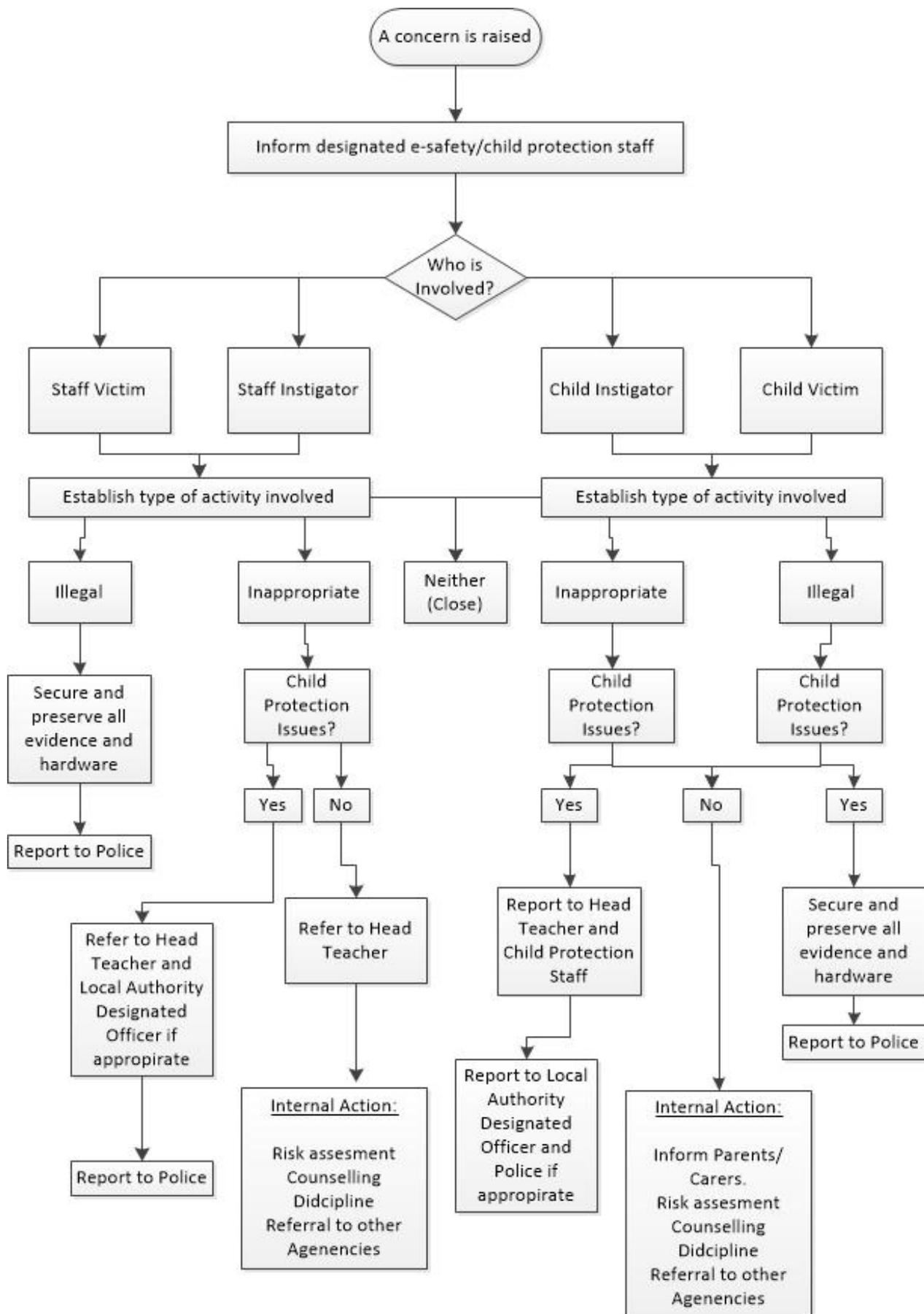
Unsuitable/inappropriate activities

College ICT systems are only to be used for agreed, appropriate and suitable work related activities. Internet activity which is considered unsuitable or inappropriate will not be allowed and if discovered will lead to disciplinary action. Internet activity which is illegal will be reported and could lead to criminal prosecution.

Responding to incidents of misuse

It is hoped that all members of the college community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place accidentally, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of an e-safety incident it is important that there is a considered, coordinated and consistent approach. Incidents will be managed using the incident flow chart on the following page.



All incidents will be recorded and reported to the relevant parties and organisations.

Archbishop Beck Catholic Sports College Students Acceptable Use Policy Agreement

New technologies have become integral to the lives of children and young people in today's society, both within colleges and in their lives outside college. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. 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 college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The college 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.

Acceptable Use Policy Agreement

I understand that I must use college 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 college will monitor my use of the ICT systems, email and other digital communications.
- I will not share my username and password – nor will I try to use any other person's username and password.
- I will be aware of communicating on-line with unknown people may be dangerous.
- I will not disclose or share personal information about myself or others when 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 college 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 college ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting unless I have permission of a member of staff to do so.
- I will not steal, disable or cause any damage to college 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 college has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the college:

- I will only use my personal hand held/external devices (mobile phones / USB devices etc) in college if I have permission. I understand that, if I do use my own devices in college, I will follow the rules set out in this agreement, in the same way as if I was using college 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 not use chat and social networking sites, apart from within the college's VLE.

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 college:

- I understand that the college 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 college and where they involve my membership of the college 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. This may include loss of access to the college network/internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.

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 college ICT systems.

Student Acceptable Use Agreement Form

This form relates to the Student Acceptable Use Policy (AUP), to which has been explained to me in assembly.

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 college ICT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the college ICT systems and equipment (both in and out of college)
- I use my own equipment in college (when allowed) e.g. mobile phones, tablets, cameras etc
- I use my own equipment out of college in a way that is related to me being a member of this college e.g. communicating with other members of the college, accessing college email, VLE, website etc.

Name of Student _____

Signed by student _____

Date _____

Archbishop Beck Catholic Sports College

Visitor/Staff/Volunteer Acceptable Use Policy Agreement

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

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of ICT in their everyday work.

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

Acceptable Use Policy Agreement

I understand that I must use college 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 / 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 college will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of college ICT systems (eg laptops, email, VLE etc) out of college.
- I understand that the college 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 college.
- 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 college 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 their permission and in accordance with the college'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 (e.g. on the college website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students and parents/carers using official college systems. Any such communication will be professional in tone and manner
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The college and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the college:

- When I use my personal hand held/external devices (PDAs/laptops/mobile phones/USB devices etc.) in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules set by the college about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not use personal email addresses on the college ICT systems.
- 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 will ensure that my data is regularly backed up, in accordance with relevant college policies.
- 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 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 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 disable or cause any damage to college equipment, or the equipment belonging to others.
- 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 college 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.

When using the internet in my professional capacity or for college 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 college:

- I understand that this Acceptable Use Policy applies not only to my work and use of college ICT equipment in college, but also applies to my use of college ICT systems and equipment out of college and my use of personal equipment in college or in situations related to my employment by the college.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the college ICT systems (both in and out of college) and my own devices (in college and when carrying out communications related to the college) within these guidelines.

Staff/Volunteer Name _____

Signed _____

Date _____

Parent/Carer Acceptable Use Policy Guidance

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. 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 college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of E-safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

The college 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.

As parent/carers I give permission for my son/daughter to have access to the internet and to ICT systems at college, if I have any reservations I will contact the E Safety Co-ordinator Mr David Martin.

I know that my son/daughter has signed an Acceptable Use Agreement and has received, or will receive, E-safety education to help them understand the importance of safe use of ICT – both in and out of college.

I understand that the college will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the college cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the college will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will inform the college if I have concerns over my child's E-safety.

