KING EDWARD VI COMMUNITY COLLEGE
ONLINE SAFETY POLICY

Approved and adopted by the Governing Body: JULY 2015

Due for Review: JULY 2016

If this is a printed version of this policy it may not be the current version. Please source this policy electronically from the staff policy folder for the most up to date version.

KEVICC

E-SAFETY POLICY

1. Background/Rationale

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 use of these exciting and innovative tools in College and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the College. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss or sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet
- The sharing or distribution of personal images without an individual's consent or knowledge
- Inappropriate communication or contact with others, including strangers
- Cyber-bullying
- Access to unsuitable video or 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 off-line world, thus this policy is used in conjunction with other college policies (e.g. Behaviour Management and Child Protection).

As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good educational provision to build students' resilience to the risks to which they may be exposed so that they have the confidence and skills to face and deal with these risks.

2. Scope of the Policy

This policy applies to all members of the College community (including staff, students, governors, volunteers, parents/carers, visitors, community users) who have access to and are users of 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 the behaviour management policy and will inform parents/carers of incidents of inappropriate e-safety behaviour.

3. Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the College at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain College business related information; to confirm or investigate compliance with College policies, standards and procedures; to ensure the effective operation of College ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the e-mail or voice-mail account where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 1998, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

Please note that personal communications using College ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

4. Roles and Responsibilities

4.1 Governors: Governors are responsible for the approval of the E-Safety Policy and for reviewing its effectiveness. A member of the Governing Body has taken on the role of E-Safety Governor.

4.2 Principal and Senior Leaders: The Principal and other members of the Senior Leadership Team are aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

4.3 The College E-Safety Coordinator will work closely with the Senior Designated Officer for child protection. The E-Safety Coordinator will:

- take day to day responsibility for e-safety issues and a leading role in establishing and reviewing the College e-safety policies/documents
- ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place
- provide training and advice for staff
- liaise with College ICT technical staff

- receive reports of e-safety incidents and create a log of incidents to inform future e-safety developments
- report regularly to the Senior Leadership Team.

4.4 Network Manager/Technical staff are responsible for ensuring:

- that the College's ICT infrastructure is secure and is not open to misuse or malicious attack
- that users may only access the College's networks through a properly enforced password protection policy
- that the use of the network is regularly monitored as far as possible in order that any misuse can be reported to the E-Safety Coordinator for investigation and action where necessary
- that monitoring software systems are implemented and updated as agreed in College policies.

4.5 College Staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current College E-Safety policy and practices
- they have read, understood and signed the College Staff Acceptable Use Policy (see Annex A)
- they report any suspected misuse or problem to the E-Safety Coordinator for investigation and action
- digital communications with students should be on a professional level and only carried out using official College systems
- students understand and follow the College E-Safety and Acceptable Use Policy (See Annex B)
- they monitor ICT activity in lessons and extra-curricular and extended College activities
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current College policies with regard to these devices
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

4.6 The designated person for child protection is trained in e-safety issues and is aware of the potential for serious child protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying.

4.7 Students are responsible for using the College ICT systems in accordance with the Student Acceptable Use Policy (see Annex B), which they will be expected to sign before being given access to College systems.

4.8 Parents/Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in an appropriate way. The College will therefore take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website and information about e-safety campaigns and literature

5 Policy Statements

5.1 Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in e-safety is therefore an essential part of the College's e-safety provision. Students need the help and support of the College to recognise and avoid safety risks and build their resilience.

E-Safety education will be provided in the following ways:

- a planned e-safety programme will be provided as part of the ICT and PSHE curriculum – this will cover both the use of ICT and new technologies in College and outside College
- key e-safety messages in assemblies and tutorial activities
- students are taught in all lessons to be critically aware of the content they access on-line and are guided to validate the accuracy of information
- e-safety awareness weeks throughout the academic year

5.2 Staff learning

- a planned programme of e-safety training will be made available to staff. It is expected that some staff will identify e-safety as a training need within the performance management process.
- all new staff receive e-safety training as part of their induction programme, ensuring that they fully understand the College's E-Safety policy and Acceptable Use Policies
- the E-Safety Coordinator will provide advice, guidance and training as required to individuals

5.3 Governors Training – Governors

Training and awareness sessions are made available to any Governor who wishes to take part.

5.4 Technical – infrastructure/equipment, filtering and monitoring

The College ICT systems are managed in ways that ensure that the College meets the e-safety technical requirements. There are regular reviews and audits of the safety and security of College ICT systems servers, wireless systems and cabling are securely located and physical access restricted.

- all users have clearly defined access rights to College ICT systems
- all users are provided with a username and password by the Network Manager
- Users will be responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security
- the "master/administrator" passwords for the College ICT system, used by the Network Manager are available to the Principal and kept in a secure place.

- the College maintains and supports the managed filtering service provided by SWGFL
- College Infrastructure and individual workstations are protected by up to data virus software
- personal data should not be sent over the internet or taken off the College site unless safety encrypted or otherwise secured. Staff who need to do this in their particular role have their laptops encrypted

5.5 Curriculum

- E-safety is a focus in all areas of the curriculum and staff reinforce e-safety messages in the use of ICT across the curriculum
- in lessons where internet use is pre-planned, students are guided to sites checked as suitable for their use
- where students are allowed to freely search the internet, staff are vigilant in monitoring the content of websites visited
- it is accepted that from time to time, for good educational reasons, staff may need to research topics (e.g racism, drugs, discrimination) that normally result in internet searches being blocked. In such a situation, staff can request that the Network Manager distribute SWGFL log-ons for teachers to use to access the sites. Any request to do so, is audited with clear reasons for the need
- students are taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information

5.6 Use of mobile devices – e.g. mobile phone, smart phones and tablets

- Students may bring a mobile phone to school with them on condition that the phone is switched off (not placed on silent) and kept out of sight in the student's bag (not in their pockets). This applies at all times when the student is on school premises.
- When a student is seen with a mobile phone on the school premises or walking around with one that is visible in their pockets, they will have it confiscated from them. If a student's phone cannot be seen but nevertheless is heard to ring or emit a text message alert sound whilst on school premises a member of staff will require the student to hand over the phone for confiscation, as above.
- They will be able to collect their phone at the end of the day.
- The only exception to the prohibition of use of a mobile phone on school premises would be if a member of staff gives a student permission to use his or her phone at a particular time and location.
- In accordance with the School's *Internet Acceptable Usage Policy* and *E -Safety Policy*, the School reserves the right to search the content of a confiscated device where there is a reasonable suspicion that it may contain undesirable material.
- This policy will operate in conjunction with other policies including the *E-Safety Policy* and *Internet Acceptable Usage Policy*.
- It is recognised that these documents must be reviewed and revised regularly in response to developments on technology.

5.7 Use of digital and video images – Photographs and Video

- When using digital images, staff should inform and educate students/pupils about the risks associated with the taking, use, sharing, publication and distribution of images. In particular

they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites

- Staff are allowed to take digital/video images 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 should be taken when taking digital/video images that students/pupils 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
- Photographs published on the website, or elsewhere that include students/pupils will be selected carefully and will comply with good practice guidance on the use of such images
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs
- parents or carers are given the opportunity to withdraw photographs of students that are published on the College website

5.8 Data Protection

See Data Protection Policy

5.9 Communications

When using communication technologies the College considers the following as good practice:

- the official College email service may be regarded as safe and secure. Users need to be aware that email communications may be monitored (see section 3 above)
- users must immediately report, to the nominated person – in accordance with the College policy, 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 and students or parents/carers (email, VLE etc.) must be professional in tone and content.

5.10 Unsuitable/inappropriate activities

Users shall not visit internet sites, post, download, upload, communicate or pass on, material and comments that contain or relate to:

- offensive materials: child sexual abuse images, promotion or conduct or illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation, adult material that potentially breaches the Obscene Publications Act in the UK, racist material, pornography, promotion of any kind of discrimination, promotion of religious hatred, threatening behaviour
- using College systems to run a private business
- use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the College

- uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- creating or propagating computer viruses or other harmful files
- carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the internet
- this also applies to personal handheld technologies whilst on College premises.

5.11 Responding to incidents of misuse

Any apparent or actual misuse which appears to involve illegal activity i.e

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- other criminal conduct, activity or materials will be reported initially to the E-Safety Coordinator

Actions will be followed in line with the College procedures including reporting the incident to the police and the preservation of such evidence.

It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. Such incidents of misuse will be dealt with through the normal Behaviour for Learning Policy.

6 Review of Policy

This policy is reviewed by the Governing Body on an annual basis.

Signature of Principal and Chair of Governors

Principal

Chair of Governors

Policy approved by the governing Body

The Policy will be reviewed in November 2015

ANNEX A

Staff and Volunteer Acceptable Use Policy

College Policy

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. 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;
- that 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 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 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 (e.g. laptops, email, VLE, social networks 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 including students 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 use chat and social networking sites in College in accordance with the College's policies;
- I will only use chat and social networking facilities supplied by the Colleges virtual learning platform or other professional teaching bodies. I will not access and use any other chat and social websites;
- 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 make available any personal email addresses / mobile phones numbers / social networking sites for such communications with students and parents / carers;
- I will not engage in any on-line activity that may compromise my professional responsibilities;

Access to the college's Management Information System is only accessible to those staff members or individuals working on behalf of the college who require it. Usage of the college's Management Information System is subject to the following:

- I understand that, in the course of my duties I may come across information of a sensitive nature. I will not disclose, under any circumstances, confidential College information, student information or data of a sensitive nature relating to individual students to any unauthorised parties;
- I will change my password to the MIS system in accordance with the local authority and College password policy;
- I will lock the screen before moving away from any computer I am using during the normal working day, to prevent unauthorised access;
- I will only store confidential College information, student information or data of a sensitive nature on a device which is encrypted or protected with a strong password;
- I am aware that any student information displayed on the screen may also be displayed on the whiteboard if the projector is turned on. I will ensure that projectors are turned off the screen, the screen is frozen or disconnected before using the MIS system, to access any confidential College information, student information or data of a sensitive nature relating to individual students;
- I will not send any confidential College information, student information or data of a sensitive nature via the internet, without the Data Protection Officer's approval;
- I will ensure printed hard copies of confidential College information, student information or data

of a sensitive nature are securely stored and disposed of after use, in accordance with College policy;

Where you are working at home and connect remotely to the college's Management Information System then all of the above considerations also apply. You must ensure that your home Internet connection is secure from outside access particularly if a wireless network is used.

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, unless this is allowed in College policies;
- I will not disable or cause any damage to College 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 College / LA Personal Data Policy. Where personal data is transferred outside the secure College 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 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).

Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Staff and Volunteer ICT Acceptable Use Agreement.

If you do not sign and return this agreement, access will not be granted to College ICT systems.

Staff and Volunteer Acceptable Use Policy Agreement

I have read and understand the above and agree to use the College ICT systems within these guidelines.

- 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 verbal warning, a written warning, a suspension, referral to Governors and / or the Local Authority and in the event of illegal activities the involvement of the police.

Staff / Volunteer Name:	
Signed:	
Date:	

ANNEX B

Enhanced Student Acceptable Use
Policy Agreement (Portable devices)

Please read through this document carefully and complete the form, acknowledging that you have understood and agree to the rules included in the agreement. If you do not sign and return this agreement, access will not be granted to the college ICT systems.

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. In order to ensure the availability of the systems, the network resources must be securely managed.

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 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 be aware of "stranger danger", when I am communicating on-line;
- I will not disclose or share personal information or images, 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 (e.g. YouTube), unless I have permission of a member of staff to do so;
- I will make sure that files I bring in on removable media (such as floppy disks, CDs, flash drives etc.) will be checked with antivirus software and I will only use them if they are found to be clean of viruses;

I will act as I expect others to act towards 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 will respect other users and will not harass, harm, offend or insult others.

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 (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 not intentionally damage, disable or otherwise interfere with the operation of computers.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will only print work required for college, and I will carefully check my work before printing and not waste resources by printing more than I need
- 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 facilities supplied by the colleges' virtual learning platform with permission and at the times that are allowed. I will not access and use any other chat and social websites.
- I will protect the computers from spillages and damage by not eating or drinking in any room containing computers.

When using the internet, I recognise that:

- I will only access the internet for study or college authorised activities.

- I should ensure that I have permission to use the original work of others in my own work
- I will respect the work and ownership rights of people outside the college, as well as other students or staff. I will not download files which are protected by copyright (including images, 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 will not use the internet to obtain, download, send, print, display or otherwise transmit materials which are unlawful, obscene or abusive.

When I am using college email for communication :

- I will not open any attachments to emails, unless I know and trust the person / organisation that sent the email, due to the risk of the attachment containing viruses or other harmful programmes.
- I will not send global emails or SPAM
- I will not access other webmail sites
- If I receive an email containing material of a violent, dangerous, racist or inappropriate nature I will report it to network services or my teacher. I will not send or promote an email containing anything which could offend others.

When I use my portable 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 not use any portable device in the classroom **without the express permission of the teacher**;
- I will take full responsibility for any portable device that I use and understand that the college will not take any **financial responsibility for its loss**. In addition, I understand that the college bears **no responsibility for confiscated items** under the terms of this policy;
- I will use my portable device responsibly so that it is not used in any manner or place that is disruptive to the normal routine of the college;
- I will ensure that any wireless password key is not shared with others and is changed periodically in line with the college's password policy;
- I will lock the screen, using appropriate security, before moving away from any portable device I am using during the normal college day, to prevent unauthorised access;
- 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 wireless network;
- 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) 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 which are 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 disable or cause any damage to college equipment, or the equipment belonging to others, through the use of my own portable device;
- I will not wear head phones connected to mobile devices during lessons unless a teacher gives me permission;

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 as described in the college behaviour policy. This may include loss of access to the college network / internet, student behaviour log, detentions, suspensions, contact with parents and, in the event of illegal activities, involvement of the police.

Use of digital/Video Images

The use of digital / video images plays an important part in learning activities. Students and members of staff may use digital cameras to record evidence of activities in lessons and out of college. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the college website and in the public media,

The college will comply with the Data Protection Act 1988 and request parents / carers permission before taking images of members of the college. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents are requested to sign the permission form below to allow the college to take and use images of their children.

Enhanced Student Acceptable Use Policy Agreement (Portable devices)

Enhanced Student Acceptable Use Agreement Form (Portable Devices)

This form relates to the student Acceptable Use Policy (AUP), to which it is attached.

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 out of college in a way that is related to me being a member of this college eg communicating with other members of the college, accessing college email, VLE, website etc.
- I will take full responsibility for any portable device that I use and understand that the college will not take any **financial responsibility for its loss**. In addition, I understand that the college bears **no responsibility for confiscated items** under the terms of this policy;

Name of Student (Capital letters)

Forename	
Surname	
Tutor Group	
Student Signature	Date
Parent/Carer signature	Date

As the parent / carer of the above student, I agree to the college taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the college.

I agree that if I take digital or video images at, or of, college events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Parent/Carer Signature	Date