School Policies

Policy title	E-Safety Policy

Written by	C Bailey	Reviewed on	OCT 2018	Next review due	OCT 2019
SLT link	jfo		Governor link	Mary Pantling	

Copies in	Policies folder X	Handbook	Student planner	Website X
Signed	Chair Governors			

This Policy covers the use of ICT systems, equipment and software (in and out of College), using personal equipment in College, cyber-bullying, Data protection, passwords and security, digital images / video images, mobile/hand-held devices (cf Electronic Devices Policy) and the College's responsibility and commitment to take action over College-related e-safety incidents (cf Safeguarding Policy and Prevent Protocol)

Contents

1. Introduction and Overview

Rationale

The purpose of this policy is to ensure all users understand their roles in promoting safe and effective uses of Information Technologies and to;

- Set out the key principles expected of all members of the College community at Crown Hills Community College with respect to the use of ICT-based technologies.
- Safeguard and protect the children and staff of Crown Hills Community College.
- Assist College staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- Set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- Have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other College policies.
- Ensure that all members of the College community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- Minimise the risk of misplaced or malicious allegations made against adults who work with students.

The main areas of risk for our College community can be summarised as follows:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- hate sites
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation

- health and well-being (amount of time spent online (internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

(Ref Ofsted 2013)

Scope

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

The Education and Inspections Act 2006 empowers Headteachers / Principals 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 outside of the College, but is linked to membership of the College. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

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 out of College.

Role	Key Responsibilities
Principal	• To take overall responsibility for e-Safety provision • To take overall responsibility for data and data security • To ensure the College uses an approved, filtered Internet Service, which complies with current statutory requirements • To be responsible for ensuring that staff receive suitable training to carry out their e-safety roles and to train other colleagues, as relevant • To be aware of procedures to be followed in the event of a serious e-Safety incident • To receive regular monitoring reports from the E-Safety Co-ordinator / Officer • To ensure that there is a system in place to monitor and support staff who carry out internal e-safety procedures(e.g. network manager)

Role	Key Responsibilities

e-Safety Co-ordinator / Designated Child Protection Lead	• To take day to day responsibility for e-safety issues and has a leading role in establishing and reviewing the College e-safety policies / documents
	• To promote an awareness and commitment to e-safeguarding throughout the College community
	• To ensure that e-safety education is embedded across the curriculum
	• To liaise with College ICT technical staff
	• To communicate regularly with SLT and the designated e-Safety Governor / committee to discuss current issues, review incident logs and filtering / change control logs
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
	• To ensure that an e-Safety incident log is kept up to date
	• facilitates training and advice for all staff
	• To liaise with the Local Authority and relevant agencies
	• To be regularly updated in e-safety issues and legislation, and be 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 and use of social media

Governors / E-safety governor	• To ensure that the College follows all current e-Safety advice to keep the children and staff safe • To approve the E-Safety Policy and review the effectiveness of the policy. This will be carried out by the Governors / Governors Sub Committee receiving regular information about e-safety incidents and monitoring reports. A member of the Governing Body has taken on the role of E-Safety Governor • To support the College in encouraging parents and the wider community to become engaged in e-safety activities • The role of the E-Safety Governor will include: • regular review with the E-Safety Co-ordinator / Officer (including e-safety incident logs, filtering / change control logs)
Computing Curriculum Leader	• To oversee the delivery of the e-safety element of the Computing curriculum • To liaise with the e-safety coordinator regularly

Role	Key Responsibilities
Education Technologist	• To report any e-Safety related issues that arises, to the e-Safety coordinator. • To ensure the College's policy on web filtering is applied and updated on a regular basis • To keep up to date with the College's e-safety policy and technical information in order to effectively carry out their e-safety role and to inform and update others as relevant
Network Provider	• To ensure that users may only access the College's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date) • To ensure the security of the College ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on College-owned devices • that the use of the network (/ remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the E-Safety Co-ordinator • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster • To keep up-to-date documentation of the College's e-security and technical procedures
Data Manager	• To ensure that all data held on students on the College office machines have appropriate access controls in place
Teachers	• To embed e-safety issues in all aspects of the curriculum and other College activities • To supervise and guide students carefully when engaged in learning activities involving online technology (including, extra-curricular and extended College activities if relevant) • To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws

Role	Key Responsibilities
All staff All staff contd/	• To read, understand and help promote the College's e-Safety policies and guidance • To read, understand, sign and adhere to the College staff Acceptable Use Agreement / Policy • To be 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 • To report any suspected misuse or problem to the e-Safety coordinator • To maintain an awareness of current e-Safety issues and guidance e.g. through CPD • To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with students should be on a professional level and only through College based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Students	• To read, understand, sign and adhere to the Student Acceptable Use Policy • To have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • To understand the importance of reporting abuse, misuse or access to inappropriate materials • To know what action to take if they or someone they know feels worried or vulnerable when using online technology. • To know and understand College Electronic Devices policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand College policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's E-Safety Policy covers their actions out of College, if related to their membership of the College • To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in College and at home • To help the College in the creation/ review of e-safety policies
Parents/carers	• to support the College in promoting e-safety and endorse the Parents' Acceptable Use Agreement which includes the students' use of the internet and the College's use of photographic and video images • to read, understand and promote the College Pupil Acceptable Use Agreement with their children • to access the College website / on-line student / pupil records in accordance with the relevant College Acceptable Use Agreement. • to consult with the College if they have any concerns about their children's use of technology

Role	Key Responsibilities
External groups	• Any external individual / organisation will sign an Acceptable Use Policy prior to using any equipment or the internet within College

Communication:
How the policy will be communicated to staff/students/community in the following ways:

- Policy to be posted on the College website and Handbook
- Policy to be part of College induction pack for new staff
- Acceptable use agreements discussed with students at the start of each year
- Acceptable use agreements to be issued to whole College community, usually on entry to the College
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The College will take all reasonable precautions to ensure e-Safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a College computer or mobile device. Neither the College nor the Local Authority can accept liability for material accessed, or any consequences of Internet access

- Staff and students are given information about infringements in use and possible sanctions. The sanctions available include:
  - interview/counselling by teacher / Behaviour Support / e-Safety Coordinator / Principal;
  - informing parents or carers;
  - seclusion or exclusion from school;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to LA / Police.

- Our e-Safety Coordinator acts as first point of contact for any complaint. Any complaint about staff misuse is referred to the Principal.

- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with College / LA child protection procedures.

Review and Monitoring

The e-safety policy is referenced from within other College policies: Safeguarding Child Protection policy, Electronic Devices policy, Anti-Bullying policy, Behaviour Policy and in the College Improvement Plan and Safer Care Code of Conduct.

- The e-safety policy has been written by the College e-safety Coordinator and is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the SLT and approved by Governors. All amendments to the College e-Safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil e-Safety curriculum

This College

- Has a clear, progressive e-safety education programme as part of the Computing curriculum / PSHE curriculum. This covers a range of skills and behaviours appropriate to their age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a web site / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - to understand why and how some people will 'groom' young people for sexual reasons;
    - to understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - to recognise the dangers posed by radicalisation online
    - to know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Policy which every student will sign/will be displayed throughout the College/will be displayed when a student logs on to the College network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.
- Ensures that when copying materials from the web, staff and students understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and students understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include, risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and governor training

This College

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on e-safety issues and the College's e-safety education programme
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the e-Safeguarding policy and the College's Acceptable Use Policies
- Ensures all staff complete safeguarding training which includes e-safety.

Parent awareness

This College

- Provides guidance for parents
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - in College newsletters; on the College web site;
    - demonstrations, practical sessions held at College;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this College, all users:

- are responsible for using the College ICT systems in accordance with the relevant Acceptable Use Policy which they will be expected to sign before being given access to College systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- should understand the importance of adopting good e-safety practice when using digital technologies out of College and realise that the College's E-Safety Policy covers their actions out of College, if related to their membership of the College. This is contained within the Safer Code of Conduct guidance document
- will be expected to know and understand College policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand College policies on the taking / use of images and on cyber-bullying

Incident Management

In this College:

- there is strict monitoring and application of the e-safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively
- support is actively sought from other agencies as needed (eg the Local Authority, the provider and regional broadband grid,) in dealing with e-safety issues
- monitoring and reporting of e-safety incidents takes place and contribute to developments in policy and practice in e-safety within the College. The records are reviewed/audited and reported to the College's senior leaders, Governors / PREVENT / the LA / the Safeguarding Board
- Any data breach (e.g lost data, theft of equipment, lost device, security issue etc) will be reported on a Security Breach Report form
- parents / carers are specifically informed of e-safety incidents involving young people for whom they are responsible
- We will contact the Police if one of our staff or students receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure and network / internet access

This College:

- Utilises a managed IT service. The provider ensures that the system meets all LA and contractual requirements including performance, backups, access, security (for users and guests, password security and routines, email accounts and KPIs)
- Has educational filtered secure broadband through EMPSN
- Uses the Capita OpenHive filtering system which blocks sites that fall into categories such as pornography, race hatred, gaming, sites of an illegal nature, etc. All changes to the filtering policy are logged and only available to staff with the approved 'web filtering management' status;
- Blocks all Chat rooms and social networking sites except those that are part of an educational network or approved Learning Platform eg Sharepoint
- Ensures students only publish within an appropriately secure environment : the College's learning environment or approved Educational network or applications eg Edmodo
- Requires staff to preview websites before use and plans the curriculum context for Internet use to match students' ability
- Uses teacher 'remote' management control tools for controlling workstations / viewing users / setting-up applications and Internet web sites, where useful;
- Storage of all data within the College will conform to the UK data protection requirements

  Students and Staff using mobile technology, where storage of data is online, will conform to the EU data protection directive where storage is hosted within the EU.

- Makes clear that no one should log on as another user and makes clear that students should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network
- Requires all users to always log off when they have finished working or are leaving the computer unattended
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves.
- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the College is used according to the Policy
- Has integrated curriculum and administration networks, but access to the Management Information System is set-up so as to ensure staff users can only access modules related to their role
- Does not allow any outside Agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems;
  e.g. technical support or MIS Support, our Education Welfare Officers accessing attendance data on specific children, parents using a secure portal to access information on their child;
- Uses our broadband network for our CCTV system and have had set-up by approved partners;
- Uses the DfE secure s2s website for all CTF files sent to other Colleges;
- Ensures that all pupil level data or personal data sent over the Internet is encrypted or only sent within the approved secure system in our LA

Students:

- Students are introduced to, and use e-mail as part of the ICT/Computing scheme of work.
  - not to delete malicious of threatening e-mails, but to keep them as evidence of bullying;
  - not to arrange to meet anyone they meet through e-mail without having discussed with an adult and taking a responsible adult with them;
  - that forwarding 'chain' e-mail letters is not permitted.

Staff:

- Never use email to transfer staff or pupil personal data.
- Staff know that e-mail sent to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on College headed paper.
  - the sending of chain letters is not permitted;

College website

- The Principal takes overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained
- Uploading of information is restricted to our website authorisers
- The College web site complies with the statutory DfE guidelines for publications
- Most material is the College's own work; where other's work is published or linked to, we credit the

sources used and state clearly the author's identity or status

- The point of contact on the web site is the College address, telephone number and we use a general email contact address; office@crownhills.leicester.sch.uk Home information or individual e-mail identities will not be published
- Photographs published on the web do not have full names attached
- We do not use students' names when saving images in the file names or in the tags when publishing to the College website
- We do not use embedded geodata in respect of stored images
- We expect teachers using' College approved blogs or wikis to password protect them and run from the College website

Learning platform / Sharepoint

- Uploading of information on the Colleges' Learning Platform / virtual learning space is shared between different staff members according to their responsibilities e.g. all class teachers upload information in their class areas
- Photographs and videos uploaded to the College's LEARNING PLATFORM will only be accessible by members of the College community
- In College, students are only able to upload and publish within College approved and closed systems, such as the Learning Platform

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the Colleges' preferred system for such communications
- The College's preferred system for social networking will be maintained in adherence with the communications policy.

College staff will ensure that in private use:

- No reference should be made in social media to students / students, parents / carers or College staff
- They do not engage in online discussion on personal matters relating to members of the College community
- Personal opinions should not be attributed to the College or local authority
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

Video Conferencing

This College

- Only uses approved or checked webcam sites;

CCTV

- We have CCTV in the College as part of our site surveillance for premises, staff and student safety. We

will not reveal any recordings (*retained by the Support Provider for 28 days*), without permission except where disclosed to the Police as part of a criminal investigation.

- We may use audio or video lesson recording equipment on occasions as a tool to share best teaching practice. We do not reveal any such recordings outside of the staff and will not use for any other purposes.

5. Data security: Management Information System access and Data transfer

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into College are entirely at the risk of the staff member, student, parent or visitor. The College accepts no responsibility for the loss, theft or damage of any phone or hand held device brought into College
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided; except where it has been explicitly agreed otherwise by the Principal. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Principal is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary
- The College reserves the right to use its statutory right search the content of any mobile or handheld devices on the College premises where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence, extremism or bullying. Staff mobiles or hand held devices may be searched at any time as part of routine monitoring
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- If a student breaches the College policy on Electronic Devices then the phone or device will be confiscated and will be held in a secure place in the College office. Mobile phones and devices will be released to parents or carers in accordance with the College 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
- 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 personally-owned devices and will be made aware of boundaries and consequences
- Students will be provided with College devices to use in specific learning activities under the supervision of a member of staff.

Staff use of personal devices

- Staff will be issued with a College phone where contact with students, parents or carers is required
- Staff should not use personally-owned 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 College policy then disciplinary action may be taken

Digital images and video

In this College:

- We gain parental / carer permission for use of digital photographs or video involving their child as part of the College agreement form when their daughter / son joins the College;
- We do not identify students in online photographic materials or include the full names of students in the credits of any published College produced video materials / DVDs;
- Staff sign the College's Acceptable Use Policy and this includes a clause on the use of mobile phones / personal equipment for taking pictures of students;
- If specific pupil photos (not group photos) are used on the College web site, in the prospectus or in other high profile publications the College will obtain individual parental or pupil permission for its long term use
- Students are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.

Asset disposal

Details of all College-owned hardware will be recorded in a hardware inventory.

Details of all College-owned software will be recorded in a software inventory.

All redundant equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

All redundant equipment that may have held personal data will have the storage media forensically wiped. Alternatively, if the storage media has failed, it will be physically destroyed. The College will only use authorised companies who will supply a written guarantee that this will happen

Disposal of any equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

ICT Acceptable Use Policy - Students

School Policy

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 school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

Acceptable Use Policy Agreement

I understand that I must use school ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

For my own personal safety:

• I understand that the school will monitor my use of the ICT systems, email and other digital communications.

• I will treat my username and password like my toothbrush – I will not share it, nor will I try to use any other person's username and password.

• I will be aware of "stranger danger", when I am communicating on-line.

• I will not disclose or share personal information about myself or others when on-line.

• If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me.

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line.

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

• I understand that the school ICT systems are primarily intended for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not use the school ICT systems for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

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

• I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

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

• I will only use my personal hand held / external devices (mobile phones / USB devices etc) in school if I have permission. I understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings.

• I will only use chat and social networking sites with permission and at the times that are allowed

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

• I should ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not try to download copies (including music and videos)

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

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

• I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the school network / internet, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.