Hamble Community Sports College

e-SAFETY POLICY

CONTENTS

1. INTRODUCTION

Information, Communication Technology (ICT) in the 21st Century is seen as an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, Hamble Community Sports College needs to build in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment.

ICT covers a wide range of resources including; web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT within our society as a whole. Currently the internet technologies children and young people are using include:

- ☐ Websites
- ☐ Learning Platforms and Virtual Learning Environments
- ☐ E-mail and Instant Messaging
- ☐ Chat Rooms and Social Networking
- ☐ Blogs and Wikis
- ☐ Pod casting
- ☐ Video Broadcasting
- ☐ Music Downloading
- ☐ Gaming
- ☐ Mobile/Smart phones with text, video and/ or web functionality
- ☐ Other mobile devices with web functionality

Whilst exciting and beneficial much ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these Internet technologies.

At Hamble Community Sports College, we understand the responsibility to educate our students on e-Safety issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

This policy and the Acceptable Use Agreements are inclusive of fixed and mobile internet technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, voting systems, digital video equipment, etc.) and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, camera phones, PDAs and portable media players, etc.).

2. ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Headteacher and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

e-Safety Co-ordinator

The e-Safety Co-ordinator in our school is a member of the Senior Leadership Team. All members of the school community have been made aware of who holds this post. It is the role of the e-Safety Co-ordinator to keep abreast of current issues and guidance through organisations such as CEOP (Child Exploitation and Online Protection) and Childnet. Senior Management and Governors are updated by the e-Safety Co-ordinator and all have an understanding of the issues and strategies at our school in relation to local and national guidelines and advice.

e-Safety Curriculum Manager

The e-Safety Curriculum Manager is an Assistant Head. The role of the e-Safety Curriculum Manager is to ensure that all staff are aware of the contents of this policy and that where appropriate; e-Safety is incorporated into teaching and learning.

e-Safety Network Manager

The IT Manager in our school is the e-Safety Network Manager. The role of the e-Safety Network Manager is to ensure that the school's computer network is safe for staff and students to use. This includes monitoring computer use and filtering inappropriate material and websites. The e-Safety Network Manager should report any network misuse or acceptable use agreement violations to the e-Safety Co-ordinator.

All School Staff

New staff will receive information on the school's e-Safety policy as part of their induction and are expected to sign the Staff Acceptable use agreement. All staff will be made aware of individual responsibilities relating to the safeguarding of children within the context of e-Safety and know what to do in the event of misuse of technology by any member of the school community. All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

3. E-SAFETY IN THE CURRICULUM

The aim of this policy, supported by the school's acceptable use agreements for staff, governors, visitors and students, is to protect the interests and safety of the whole school community. It is linked to the following policies: Child Protection, Health and Safety, Home/School Agreement, Behaviour and PSHCE**.** All users are expected to read and sign the relevant Acceptable Use Agreement to demonstrate that they have understood the school's e-safety policy.

The school provides opportunities within a range of curriculum areas to teach e-Safety. Students will be made aware of the following:

- ☐ Safe and acceptable use of the school network.
- ☐ Dangers of technologies that maybe encountered outside school.
- ☐ Relevant legislation when using the internet such as data protection and intellectual property, which may limit what they want to do but also, serves to protect them.
- ☐ Copyright and respecting other people's information, images, etc. through discussion, modelling and activities.
- ☐ Software copyright and licensing. It is illegal to copy or distribute school software or illegal software from other sources.
- ☐ Impact of online bullying and know how to seek help if they are affected by these
- ☐ issues. Students should also be aware of where to seek advice or help if they experience problems when using the internet and related technologies i.e. parent/carer, teacher/trusted staff member or an organisation such as Childline/CEOP report abuse button.

4. PASSWORD SECURITY

Users are provided with an individual network; e-mail and SIMS log-in username and password. They are expected to keep their passwords private. Students are not allowed to deliberately access materials or files on the school network, of their peers, teachers or others. If you think your password may have been compromised or someone else has become aware of your password report this to the e-Safety Network Manager immediately.

Staff should be aware of their individual responsibilities to protect the security and confidentiality of the school network. Individual staff users must also ensure that workstations are locked when unattended. In our school, all ICT password policies are the responsibility of the Network Manager and all staff and students are expected to comply with the policies at all times.

5. DATA SECURITY

We regard the lawful and correct treatment of personal information by the school as very important to successful operations and for maintaining confidence between ourselves and those with whom we deal. We therefore make every effort to ensure that personal information is treated lawfully and correctly.

Hamble Community Sports College needs to collect a range of personal information in order to operate. This includes current, past and prospective students, employees, supplies, clients/customers, and others with whom it communicates. The school requires this information to support the administration of contracts with these people and, in addition, it may occasionally be required by law to collect and use information of this kind to comply with the requirements of government departments, for business data, for example. This personal information must be dealt with properly however it is collected, recorded and used – whether on paper, in a computer, or recorded on other material and there are safeguards to ensure this in the Data Protection Act 1998.

We fully endorse and adhere to the principles of data protection, as detailed in the Data Protection Act 1998 (and any subsequent amending legislation). Specifically, the principles require that personal information:

- ☐ shall be processed fairly and lawfully and, in particular, shall not be processed unless specific conditions are met; hall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or these purposes; shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed;
- ☐ shall be accurate and, where necessary, kept up to date;
- ☐ shall not be kept for longer than is necessary for that purpose or these purposes;
- ☐ shall be processed in accordance with the rights of data subjects under the Act;
- ☐ shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. Therefore, Hamble Community Sports College will, through appropriate management and application of criteria and controls:

- ☐ observe fully conditions regarding the fair collection and use of information; meet its legal obligations to specify the purposes for which information is used; collect and process appropriate information, and only to the extent that it is needed to fulfil operational needs or to comply with any legal requirements;
- ☐ ensure the quality of information used;
- ☐ apply strict checks to determine the length of time the information is held;
- ☐ ensure that the rights of people about whom information is held can be fully exercised under the Act. (These include the right to be informed that processing is being undertaken; the right of access to one's personal information; the right to prevent processing in certain circumstances; the right to correct, rectify, block or erase information which is regarded as the wrong information);
- ☐ take appropriate technical and organisational security measures to safeguard personal information;
- ☐ ensure that personal information is not transferred abroad without suitable safeguards.

In addition, Hamble Community Sports College will ensure that:

- ☐ there is someone with specific responsibility for data protection in the organisation (the Data Protection Officer);
- ☐ everyone managing and handling personal information understand that they are contractually responsible for following good data protection practice;
- ☐ everyone managing and handling personal information is appropriately trained to do so;
- ☐ any third party organisation that processes data on our behalf has adequate measures in place
- ☐ and provides us with written guarantees to this effect;
- ☐ queries about handling personal information are promptly and courteously dealt with;
- ☐ methods of handling personal information are clearly described;
- ☐ a regular review and assessment is made of the way personal information is managed.

Anybody wanting to make enquiries about handling personal information should contact the Data Protection or the HR Office at the school in the first instance. The school expects all employees with access to personal information to respect the need for confidentiality and to avoid improper use or transfer of such information. Any employee, who fails to adhere to these principles, may be subject to disciplinary action.

6. MANAGING THE INTERNET

The internet is an open communication medium, available to all, at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people. Whenever any inappropriate use is detected it will be followed up.
The school maintains that students will have supervised access to Internet resources through the school's fixed and mobile internet technology.
Staff will preview any recommended sites before use.
If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.
All users must observe copyright of materials from electronic resources.

7. INFRASTRUCTURE

Hamble Community Sports College has two monitoring solutions where web-based activity is filtered, monitored and recorded. School internet access is controlled through a filtering device provided and maintained by Hampshire County Council. Staff and students are aware that school based e-mail and internet activity can be monitored and explored further if required. The school does not allow students access to internet logs. If staff or students discover an unsuitable site, the site is reported immediately to the e-safety network Manager.

It is the responsibility of the school, by delegation to the network manager, to ensure that Anti-virus protection is installed and kept up-to-date on all school machines. Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date virus protection software. It is not the school's responsibility to install or maintain virus protection on personal systems. If students wish to bring in work on removable media it must be given to the ICT technicians or teacher for a safety check first. Students and staff are not permitted to download programs on school based technologies.

8. MANAGING OTHER WEB 2 TECHNOLOGIES

Web 2/Social networking sites, if used responsibly can provide easy to use, creative and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture and commercialism. To this end, we encourage our staff and students to think carefully about the way that information can be added, viewed and removed by all users, including themselves, from these sites. At present, the school endeavours to deny access to social networking sites to students within school.

All staff and students are advised to be cautious about the information given by others on sites, for example users not being who they say they are. Staff are asked and students are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.
Staff and students are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/e-mail address, specific hobbies/ interests). Our staff and students are strongly advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals. Staff and students are encouraged to be wary about publishing specific and detailed private thoughts online. Our students are asked to report any incidents of bullying to the school. Staff may only create blogs, wikis or other web 2 spaces in order to communicate with students using the LA Learning Platform or other systems approved by the Headteacher. Staff are strongly advised not to allow students and students to access their social networking sites. Staff are strongly advised not to visit students or student's social networking sites.

9. MOBILE TECHNOLOGIES

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as portable media players, PDAs, gaming devices, mobile and smart phones are familiar to children outside of school too. They often provide a collaborative, well-known device with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately. The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/carer using their personal device. Mobile phones should not be used in the classroom for personal calls without the express permission of the Headteacher.

Under no circumstances should these devices be used to circumvent any school policy or the school internet filtering for Teaching and Learning. At no time will the school incur any costs associated with any personal devices for any reason unless with the express permission of the Headteacher.
Students are allowed to bring personal mobile devices/phones to school but they must be switched off at 8.35am and only switched back on at break and lunch. The school is not responsible for the loss, damage or theft of any personal mobile device. The sending of inappropriate text messages or files (including pictures and video via Bluetooth, infra-red, direct connection, jokes, etc.) between any members of the school community is not allowed. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device. Mobile devices (Mobile Phone/Mobile Tablet) can be used to store data including that contained in e-mail accounts. If your personal or school owned device contains school data or has a school e-mail account set up on it, then the device must have a password to gain access.

10. MANAGING E-MAIL

The use of e-mail within most schools is an essential means of communication for staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail can offer significant benefits including; direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an e-mail in relation to their age and good ‘netiquette’. In order to achieve ICT level 4 or above, students must have experienced sending and receiving e-mails.
The school gives all staff and students their own e-mail account to use for all school business. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged. This should be the account that is used for all school business. Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses. E-mail sent to an external organisation should be written carefully before sending, in the same way as a letter written on school headed paper. Staff sending e-mails to external organisations, parents or students are advised to cc. their line manager or designated account.
Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes. All e-mail users are expected to adhere to the generally accepted rules of network etiquette (netiquette) particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others.

Students must immediately tell a teacher/trusted adult if they receive an offensive e-mail.
Staff and students must inform the e-Safety network manager, if they receive an offensive e-mail.
Students are introduced to e-mail as part of the ICT Scheme of Work.

11. SAFE USE OF IMAGES

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misused. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.
With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.
Staff and students are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of Staff or students, this includes when on field trips. However, with the express permission of the Headteacher, images can be taken provided they are transferred immediately and solely to the schools network and deleted from the staff device.

Consent of Adults Who Work at the School

Permission to use images of all staff who work at the school is sought when required.

Publishing Students' Images and Work

On a child's entry to the school, all parents/guardians will be asked to give permission to use their child's work/photos in the following ways:

- ☐ on the school web site
- ☐ on the school's Learning Platform
- ☐ in the school prospectus and other printed publications that the school may produce for promotional purposes
- ☐ recorded/transmitted on a video or webcam
- ☐ in display material that may be used in the school's communal areas
- ☐ in display material that may be used in external areas, i.e. exhibition promoting the school
- ☐ general media appearances, e.g. local/national media/press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

Storage of Images

Images/films of children are stored on the school's network and on our school's website.
Students and staff are not permitted to use personal portable media for storage of images (e.g. USB sticks) without the express permission of the Headteacher. The e-Safety Co-ordinator has the responsibility of deleting the images when they are no longer required, or the student has left the school.

Webcams and CCTV

The school uses CCTV for security and safety. The only people with access to this are the ICT support and premises teams. Images and film will not be viewed by anyone else except with the express permission of the Headteacher.

12. WEB INFORMATION SEREVICES (WIS)

The Web Information services is made up of a collection of web based services that provide access to information held on college systems over the internet. These services include but not limited to Skoogle2, Hamble VPN, Parent Portal, Show My Homework, and Webmail.

System Security

This policy is intended to minimize security risks. These risks might affect the integrity of the school's data, the authorised WIS User and the individuals to which the WIS data pertains. In particular these risks arise from:

- ☐ The intentional or unintentional disclosure of login credentials to the school's Learning Gateway by authorised users.
- ☐ The wrongful disclosure of private, sensitive and confidential information.
- ☐ Exposure of the school to vicarious liability for information wrongfully disclosed by authorised users.

Data Access

This policy aims to ensure all relevant aspects of the Data Protection Act (1998) and the Fair Processing policy are adhered to. The policy aims to promote the best use of the WIS system to:

- ☐ Further the communication and freedom of information between school and parents/guardians by allowing them to view selected school information about their child.
- ☐ Allow students to view selected school information about them.
- ☐ Allow staff to access and update selected school information from outside of the school network.

Authorised Learning Gateway Users

Access to the WIS is granted only on condition that the individual formally agrees to the terms of this Policy. Hamble Community Sports College's WIS system is provided for use only by:

- ☐ Persons who are legally responsible for students currently attending the school.
- ☐ Current staff members.
- ☐ Students currently on roll.

The authorising member of school staff must confirm that there is a legitimate entitlement to access information for students, and the appropriate access request form must be signed before access is granted. A copy of the form will be held by the school for audit purposes.

Personal Use

Information made available through the WIS is confidential and protected by law under the Data Protection Act 1998. To that aim:

- ☐ Users must not distribute or disclose any information obtained from the WIS to any person(s) with the exception of the pupil to which the information relates or to other adults with parental responsibility.
- ☐ Users should not attempt to access the WIS in any environment where the security of the information contained in the Learning WIS may be placed at risk e.g. a cybercafé.

Password Policy

- ☐ You must assume personal responsibility for your username and password. Never use anyone else's username or password.
- ☐ You must always keep your individual user name and password confidential. These usernames and passwords should never be disclosed to anyone. Passwords and user names should never be shared.
- ☐ In some instances users may be given the right to change the WIS password from the one originally issued by the school. If this is the case the following rules must be followed.
- ☐ Passwords must be at least 8 characters (a-z, 0-9) in length.
- ☐ Passwords must contain at least 1 number (0-9).

- ☐ Passwords must contain at least 1 capital letter.
- ☐ Passwords must not be similar to your own name or username for example: Cutler1.

Questions, Complaints and Appeals

WIS users should address any complaints and enquiries about the Learning Gateway system to the school by e-mail: general@hamblecollege.co.uk or telephone: 02380 452105. Hamble Community Sports College reserves the right to revoke or deny access to the WIS of any individual under the following circumstances:

- ☐ The validity of parental responsibility is questioned
- ☐ Court ruling preventing access to child or family members is issued
- ☐ Users found to be in breach of the Learning Gateway usage policy
- ☐ If any child protection concerns are raised or disputes occur the school will revoke access for all parties concerned pending investigation.

Please note: Where WIS access is not available the school will still make information available according to Data Protection Act (1998) law. Users are liable for any potential misuse of the system and/or breach of the data protection act that may occur as a result of failing to adhere to any of the rules/guidelines listed in this document.

13. MISUSE AND INFRINGEMENTS

All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Network Manager.
Deliberate access to inappropriate materials by any user will lead to the incident being investigated by the e-Safety Co-ordinator, depending on the seriousness of the offence; investigation may also be undertaken by the tutor, IT Manager or Headteacher possibly leading to dismissal, suspension and involvement of the police for serious offences.

14. PARENTAL INVOLVEMENT

Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school. Parents/carers are required to make a decision as to whether they consent to images of their child being taken/used in the public domain (e.g. the school website).

Title of Policy	e-Safety Policy
Review Cycle	3 Years
Policy prepared by/Reviewed by	MBE
Committee responsible	F, P & S D
Statutory/Discretionary	Discretionary
Date of last FGB approval	09 Feb 2016
Date of last review by committee	N/A
Date of next review by FGB	Feb 2019

ACCEPTABLE USE AGREEMENT e-SAFETY RULES

STUDENT AND PARENT/CARER

ICT and the related technologies such as e-mail, the internet, portable and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all students are aware of their responsibilities when using any form of ICT. All students are expected to read and understand the schools e-Safety policy and adhere to it at all times.

The Network & Internet

- ☐ I will only use ICT systems in school, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- ☐ I will not download or install software on school computers or mobile devices.
- ☐ I will only log on to the school network/ Learning Platform with my own user name and password.
- ☐ I will follow the schools ICT security system and not reveal my passwords to anyone and change them regularly.
- ☐ I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- ☐ I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- ☐ I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- ☐ I will not give out any personal information such as name, phone number or address.
- ☐ I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- ☐ I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school into disrepute.
- ☐ I will respect the privacy and ownership of others' work on-line at all times.
- ☐ I will not attempt to bypass the internet filtering system for any reason.
- ☐ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- ☐ I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/ carer may be contacted.
- ☐ I will only enter the computer rooms when a teacher is present and when a teacher gives permission.
- ☐ I am responsible for the computer storage space available to me.
- ☐ I will treat computers with care and report any damage or malfunction immediately.
- ☐ I will not eat or drink in the computer rooms.
- ☐ I will not attempt to download/run any executable files, games, music or software from the Internet or from floppy disk, CD ROM, USB flash drive, or portable electronic device.

I will not download any music or video files unless a teacher gives express permission.

- ☐ I will not view any streaming media (video) across the internet or listen to music without the Teachers express permission.
- ☐ I will not connect to the school network any portable device – wired or wireless (including mobile phones, laptops, Media players, iPods) by any means, (WAP, WEP, Bluetooth etc.) unless specifically authorised by the ICT staff.
- ☐ I will not purchase any goods or services using the schools computers.
- ☐ Images or video of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and must not be distributed outside the school network without the permission of the Headteacher.
- ☐ Students who find anything unsuitable or inappropriate on a website or on the Open/Shared drive must report it to a teacher immediately.

E-mail

- ☐ I must keep my e-mail account secure and their password safe. I will not attempt to access another user's e-mail account and I will not allow others to use my account.
- ☐ I will not use vulgar, derogatory, or obscene language. I will not use e-mail to bully anyone, engage in personal attacks, harass another person, or give out private information about another person.
- ☐ I will not give out details about or hyperlinks to, Web sites, newsgroups, or chat areas, etc. that contain material which is obscene or inappropriate in an educational environment.
- ☐ I will not engage in "spamming" (maliciously sending an e-mail to many people at the same time) or participate in chain letters, etc.
- ☐ I will not open e-mails or attachments they could reasonably expect to contain a virus or inappropriate material, but will delete them unopened.
- ☐ The School reserves the right to filter the e-mail and inspect a Student's account if there is a suspicion that these rules have been broken.

Printing

- ☐ I am aware of the high costs of printing documents and consider keeping printing to a minimum.
- ☐ I will only print multiple copies of the same document with permission from a Teacher.
- ☐ I will avoid printing documents with a solid colour background since these are extremely expensive.
- ☐ I will only print work when a teacher gives permission.
- ☐ I will not print any material that is not school work.
- ☐ I will not print any material that could be considered offensive or illegal.
- ☐ I will not attempt to remove any paper or object 'jam' in any printer.
- ☐ I will not attempt to fill a printer with paper if it has run out unless shown how to by a member of the ICT Support Team.

ACCEPTABLE USE AGREEMENT e-SAFETY RULES

STAFF AND VISITORS

ICT and the related technologies such as e-mail, the internet, portable and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to read and understand the schools e-Safety policy and adhere to it at all times.

Personal/ Data Security

- ☐ I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- ☐ I will not give out my or others personal details such as mobile phone number and personal e-mail address to students.
- ☐ I will not store confidential material on network areas which are accessible to persons who do not have clearance to access such material.
- ☐ I will ensure that personal data such as data held on the MLE, is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely.
- ☐ I will not take students personal data off site without authorisation from the designated teacher for Child Protection / e-Safety Co-ordinator.
- ☐ I will ensure that all data taken off site, will be held securely, encrypted electronically, if appropriate, and securely destroyed on return to school.

Child Protection

- ☐ I will not allow students to use my personal or school logins for any reason.
- ☐ I am aware of the guidelines to conceal student identities when publishing to the public domain.
- ☐ I understand that students must be supervised at all times when in an ICT suite or on computer equipment.
- ☐ When arranging use of ICT facilities I will ensure that a staff member is able to monitor students at all times.
- ☐ Images of students and or staff will only be taken, stored and used for professional purposes in line with the school policy and with written consent of the parent, carer or staff member; images will not be distributed outside the school network without the express permission of the parent/ carer and the Headteacher.

Network Integrity

Before purchasing any hardware or software I will consult a member of IT staff to check compatibility, license compliance and discuss any other implications that the purchase may have.

- ☐ I will not attempt to install any software or hardware onto the school network or school owned laptops such as additional software, computer games, music or film without first discussing this with the IT staff.
- ☐ I will inform a member of the IT staff immediately of any websites accessible from within school I feel are unsuitable in any way for student consumption.
- ☐ I will inform a member of the IT staff immediately of abuse of any ICT system(s) - software and hardware - providing the location and names where possible
- ☐ I will inform a member of the IT staff immediately of any inappropriate content suspected to be on the ICT system(s). This may be contained in e-mail, documents, pictures etc.
- ☐ I will report any breaches, or attempted breaches, in security to a member of the IT staff immediately.
- ☐ I will ensure that ICT Suites are locked upon leaving the room. Students should not be allowed access to keys to ICT Suites at any time.

- ☐ Staff are responsible for all equipment and use of workstations by students during their lessons in ICT Suites. Their department will be billed for any associated damage.

Personal Integrity

- ☐ I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory. I will not store any material on the network (Home Directory or Shared areas) that is not for use within my professional role within the school.
- ☐ I will ensure that my online activity, both in school and using school equipment outside of school, will not bring my professional role into disrepute.
- ☐ I will respect copyright and intellectual property rights and will not use or make copies of any information that may breach copyright law.
- ☐ I will only use the school's e-mail/SIMS/WIS and any related technologies for professional purposes.
- ☐ I will ensure that all electronic communications with students and staff are compatible with my professional role.
- ☐ Any equipment issued to me remains the property of the school and I will take reasonable precautions to protect such equipment, including complying with insurance requirements of securing equipment at all times. The equipment is to be returned upon request or at termination of employment and is not to be passed on.
- ☐ I will support and promote the school's e-Safety policy and help students to be safe and responsible in their use of ICT and related technologies.

I understand that the right is reserved to remotely monitor and intercept network activity and my use of the Internet including e-mail and other related technologies may be monitored, logged and made available, on request, to my Line Manager or Headteacher.

I understand that any attempt to bypass the School, or other network security systems, including the introduction of viruses or applications of a destructive nature could lead to prosecution. Where it is believed that there has been a breach of legislation appropriate action will be taken.

I have read and understand my role regarding acceptable use and my role in enforcing it.
I agree to follow this code of conduct and to support the safe use of ICT throughout the School

Full Name ……

Job title ……

Signature ……

Date ……