UPLANDS COMMUNITY COLLEGE

ICT Policy

Including E-Safety and Social Media Policies

Document title	ICT Policy
Policy number	S023
Version number	1.0
Policy Status	
Date of Issue	July 2016
Date to be revised	July 2017

Revision log (last 5 changes)

Date	Version No	Brief detail of change

Contents

Vision

"To provide outstanding ICT teaching, facilities and applications across all areas of the college to equip our students with the knowledge, skills and understanding of ICT across all subject areas, so that they have the ICT capability to take them through the rest of their lives."

All students have high levels of ICT capability, able to make sensible choices about when and how to use ICT to perform a task or to enhance their learning. They use and choose hardware and software independently and appropriately and they can evaluate their choices. They appreciate the use of ICT in the wider world.

All teachers and support staff confidently exploit the use of ICT to find resources and prepare materials to enrich their lessons and to support their professional development. They are comfortable using pupil assessment and performance data to focus their objectives and planning.

The college exhibits high levels of leadership in ICT. There is a strong commitment to the resourcing (funding, time, and training) required to sustain a high level of ICT use, inside and outside the classroom.

Parents are well informed about their child's progress and behaviour, the programmes of study being followed, the marking objectives and the homework and coursework set.

Definition

Information and Communications Technology has the potential to improve the quality of teaching and learning across the Curriculum. Society is changing and there is an increasing need for a greater level of technological knowledge and awareness amongst the population as a whole to avoid the digital divide. The effective use of ICT in the classroom will help to produce a population that feels comfortable with the new technology, is able to access lifelong learning opportunities through the use of ICT and can adapt to the rapid changes in this field.

Aims

At Uplands Community College, we aim to:

- Ensure all staff and students are confident, competent and independent users of ICT;
- Motivate and inspire students and raise standards;
- Develop an appreciation of the use of ICT in the context of the wider world;
- Enrich learning and promote both autonomous study and group work;
- Develop students' ability to use ICT appropriately and choose software suitable for a particular task;
- Provide continuity and progression in all of the strands of the ICT National Curriculum;
- Develop ICT skills through curriculum contexts;
- Encourage problem-solving and investigative work;
- Foster group work, sharing and collaboration between peers;
- Care for and respect equipment;
- Share resources;
- Offer a wide range of learning possibilities to all students including a Virtual Learning Environment providing personalised learning and opportunities for individual students to accelerate their learning with the support of the college;
- Train, encourage and support teachers to exploit ICT in teaching;
- Train and encourage teachers to use the SIMS management information system;
- Develop the flexible use of new technologies (incl. wireless connections, electronic whiteboards, PDAs, tablets and video conferencing) to support and encourage a range of teaching and learning styles and opportunities;
- Make access and resources always available when required;
- Ensure that equipment is always operational.

Roles and responsibilities

The Headteacher has overall responsibility for monitoring the teaching of ICT.

The finance sub-committee ensures adequate funding is allocated to cover equipment and all necessary contracts.

The Deputy Head in charge of ICT Strategy has Leadership Responsibility for ICT across the whole college. The ICT Co-ordinator is responsible for the delivery of ICT as a discrete subject and is line manager to all teachers of discrete ICT either directly or indirectly. He/she also has overall responsibility for the ICT curriculum, teaching and learning, assessment, professional development, extended opportunities for learning, resources and impact on student outcomes within the ICT department. All Heads of Faculty are responsible for the embedding of ICT in their respective subject areas and are expected to ensure that ICT best practice is deployed in teaching across their department.

The ICT Systems Manager plans the development of the infrastructure (network, hardware, software, services) in accordance with the needs of the ICT Co-ordinator and the Deputy Head in charge of ICT Strategy. Detailed planning is carried out by the ICT Systems Manager.

The ICT Systems Manager monitors the needs of the support staff in conjunction with the Director of Finance, Business, Premises and Administration and the Deputy Head of ICT Strategy for those teachers with specific admin roles.

The ICT Co-ordinator liaises closely with the governors who have responsibility for ICT and with the curriculum sub-committee.

Special Needs and Equal Opportunities

- The college recognises the advantages of the use of ICT by students with special educational needs.

General

ICT is taught both as a discrete subject and integrated into all other curriculum areas. ICT is used as a tool to improve learning. All the schemes of work have clear ICT links where skills and techniques are carefully planned. Each subject coordinator has completed an audit of their scheme of work to ensure relevant ICT links have been included.

We aim to provide a broad and balanced curriculum through our long term ICT plans and subject schemes of work. These ensure our students are taught a range of skills and techniques in ICT as a discrete subject and as part of work in other curriculum areas.

Outside of lessons, students have access to the computer suite by arrangement during lunch break.

All the software used in college is monitored to ensure that its use is non-discriminatory and, where relevant, represents cultural diversity.

Teaching and learning

Our short-term planning operates on three levels to meet the range of our students' needs:

- All students will learn;
- Most students will progress further and learn;
- Some students will progress even further and learn.

At Key Stage 3 every lesson plan includes reference to:

- The Learning Objectives of the short term lesson plan;

- Key Processes of the New Curriculum Requirements;
- Reference to Personal, Learning, and Thinking Skills;
- Sub strands and learning objectives of the New Curriculum for the year group and progression;
- Curriculum opportunities;
- Cross-curricular links;
- Resources for the short term lesson;
- Teaching Progression;
- Details of Homework and non-ICT tasks if required due to computer failure;
- Assessment for Learning;
- SEN.

At Key Stage 3 every medium term lesson plan includes reference to;

- The Unit of Work Objectives;
- Attainment targets for levelling students;
- Student Self-Assessment;
- Teachers comment and level feedback.

Planning ensures that a wide range of strategies are employed in order to differentiate ICT tasks. Examples of these are:

- Same activity but different outcome;
- Same theme but different levels of input;
- Different pace of working;
- Different groupings of students;
- Developing different modules of work, at different times of the year, for different abilities.

Teachers' planning is reviewed by the ICT Co-ordinator to ensure staff use a range of teaching styles to develop ICT capability. The ICT Co-ordinator reviews teachers' ICT plans to ensure full coverage of the Scheme of Work and to monitor the range of teaching styles that are employed to develop ICT capability. These teaching styles include: group work of mixed and similar ability, individual work, whole class teaching. Teachers' planning will also include opportunities for work away from the computers intended to compliment the ICT activities.

Reporting and recording

Parents receive an annual written report on their child's progress in ICT. In addition to this, the college provides verbal feedback on their progress during parent interviews. At Key Stage 3 parents receive feedback on each unit of work that their children complete. Parents can also access student progress data via the college website and online portal.

Monitoring, evaluation and review

The co-ordinator monitors ICT planning each term and provides written feedback to subject co-ordinators. This ensures the scheme of work is implemented and all strands are planned for. In addition to this, the ICT co-ordinator monitors teaching and student's work on a rotational basis and copies the written feedback to both the class teacher and designated person from Leadership Team.

The Governors are kept informed of the co-ordinator's work through termly reports in the Headteacher's report to the Governors.
The scheme of work is reviewed and updated on an annual basis to ensure it reflects good practice. The scheme of work provides sufficient detail to ensure all students receive a consistent experience in ICT.

A member of Leadership Team monitors one ICT lesson per teacher each year to ensure that all classes are monitored annually.

The ICT Co-ordinator will observe ICT Teachers lessons termly.

All teachers are expected to have high expectations for all students. When monitoring ICT planning, teaching and learning due consideration is given to issues of gender and ethnicity to ensure that all students' experiences with ICT are positive.

Human resource management

The ICT curriculum will provide the main focus of one staff meeting per year. This may include introduction of software, training for ICT, whole college support in planning for ICT, sharing student's work, moderation of student's work, development of the ICT portfolio or sharing ideas of good practice.

Opportunities of training for staff are offered, wherever possible, to meet whole college needs as well as those of individual teachers. These needs may be identified as a result of monitoring or performance management reviews.

As part of Continuing Professional Development all staff are encouraged to improve necessary skills and techniques, and take up training offered by the ICT Coordinator, ICT Systems Manager, other in-house trainers and "on-the-job" providers to develop ICT competences in the classroom linked to other curriculum areas.

Staff have the advantage of using the Internet and the VLE for their own professional development by access to national developments, educational materials, and good curriculum practice.

Technical

Any faults with the computers or infrastructure are reported to ICT Support and recorded in the "electronic log". The ICT Systems Manager will keep an up to date record of how all faults are being progressed.

The ICT Systems Manager keeps a log of faults occurring to help with future replacement decisions and with discussions with the ICT technician.

Efficient deployment of ICT

Hardware – desktop computers are not expected to last longer than 5/6 years even with upgrades. Laptop computers are not expected to last longer than four years. The total number of computers required for teaching and learning is based on the courses offered and the needs of all departments, moderated by the limits of the budget. Therefore, with around 400 computers in use, we need to replace an average of 80 per year. However, acquisition was not originally uniform and the profile of computer ages is not steady. In addition, the more different varieties of model of computer the more complex is the role of the technicians supporting. The intention in the future is to acquire PCs, all of the same model, to ease support and ensure a more effective and efficient ICT infrastructure.

Utilisation of computers is monitored and a compromise is constantly sought taking into account class sizes, room capacities, consistent rooming for teachers, and access opportunities for other subjects. It is recognised that more flexible arrangements have to be sought to achieve acquisition figures in excess of 75% and for that reason we invested in a new infrastructure installation during August 2010.

Software - the majority of software is deployed to all computers where possible. Site licences are purchased unless the cost is prohibitive. This enables flexible use of rooms and facilities by different subjects and ages and means that computers can be moved from room to room without a major installation. Students get the same interface and applications on all the computers they use.

The ICT Systems Manager is responsible for ensuring that the automatic updating of anti-virus software is operating efficiently by completing a weekly check.

New software is purchased only after evaluation, whenever possible, to ensure that it fits the purpose for which it is intended, and that it is non-discriminatory.

Staff and students are not permitted to use software from external sources without prior consent from the ICT Systems Manager.

Security

The college has an alarm system installed throughout and CCTV cameras linked to a server recording external activities. The teacher should lock all computer rooms when the lesson is ended. No student is allowed in an ICT room without a teacher present. The computer suites are made secure at night as part of the college caretaker's daily routine.

Computers, projectors, televisions, video recorders, DVD players, scanners etc. are all security marked with Smart Water.

Each computer system is accessed through a password system providing security against unauthorised access to the management system. The password policy requires passwords to be changed every ninety days. Different passwords must be used for network log in and SIMS access. Passwords must contain three of:

- Upper case;
- Special character;
- Number;
- Letter.

Health and Safety

All students receive introductory sessions in dealing with Health and Safety issues. These include showing students how to adjust the brightness and contrast settings of monitors as well as the correct keyboard and seating position. Students also receive instruction on the correct procedure for using a mouse and are regularly reminded not to look directly into the projector beam when using the interactive whiteboard.

When using ICT facilities all staff will make a visual check of equipment specifically to ensure that:

-
- A fire extinguisher suitable for electrical fires is in place and undamaged;
- There are no trailing cables or leads which could constitute a health hazard;
- There are no damaged chairs or other faulty and/or potentially hazardous equipment.

Lessons involving the use of ICT should be structured to ensure that there are periodic breaks where students' attention is directed away from the monitor to a distant object such as the teacher or interactive whiteboard.

Computers located in classrooms are positioned, wherever possible, away from light reflection and glare. The optimum position is at right angles to the natural source of light.
All equipment is checked annually under the Electricity at Work Regulation 1989, and is PAT tested. A detailed inventory is kept up to date by the ICT Systems Manager, who ensures all equipment is checked. New equipment is added to the inventory on arrival.

Regular Risk Assessment surveys are conducted by the designated Health and Safety representative, faults are logged and appropriate action taken.

The Health and Safety at Work Act (1 January 1993), European Directive deals with requirements for computer positioning and quality of screens. This directive is followed for all administration staff. Whilst this

legislation only applies to people at work we seek to provide conditions which meet these requirements for all users.

Internet Safety

Key Stage 3 Unit 7.0 focuses on E-safety. Delivery of these messages is re-enforced in the PHSE scheme of work across all year groups. Unit 7.2, also delivered early in the year for year 7 focuses on reliability, validity, appropriateness, quality, and bias of information of all sources and in particular the Internet. Throughout the rest of Key Stage 3 this message is embedded in the Schemes of work.

This is enforced further by the filtering policy, Acceptable Use Policy, guidelines to teachers, letters to parents, and a number of sanctions.

Previously parents signed a letter warning of the dangers of internet access and of our inability to guarantee that inappropriate material could not be accessed, giving them the opportunity to opt their child out of unsupervised internet access. Ultimately, the aim is to make children responsible users of the internet, understanding what is and what isn't appropriate and making their own decisions accordingly. Web filters are in place to monitor access on-site and report on Internet usage. Inappropriate sites are blocked.

Management Information

The college recognises that effective use of student data can inform decisions about teaching and learning. Data is currently used for monitoring attendance, behaviour, progress, and assessment, as well as for increasing efficiency in the day to day running of the organisation.

All teaching and support staff have access to a PC through which they can access the Management Information System (MIS) at an appropriate level. All teachers have their own laptop or classroom PC available.

The procedures for protection, security, and backup of the MIS are included in the college's Information Access and Security Policy.

Personal, attendance and assessment information about each individual student are available (as a common transfer file) for the vast majority of new admissions. The local authority transmits some assessment information early, so that appropriate pathways can be devised in advance of the new intake.

Assessment

From the prior achievement records (Key Stage 2 SATS, Key Stage 3 SATS, Key Stage 4 GCSE points) of students, the Assessment Coordinator calculates the probable levels achieved by the end of the next key stage and plots way points for the end of each year. Teachers assess students against these targets three times a year, to monitor progress. The data input by the teachers is used to generate a progress report to parents, to mentor the student concerned (charts in planners) and to inform the next teacher's plans and targets.

Inclusion

All lesson plans include a note of students from vulnerable groups and suitable support, options or alternatives if appropriate. Additional use of ICT for language, literacy, and numeracy is included in programmes run by the SEN department.

Students in Flexi Learning will have access to resources on the VLE and there is computer access for these students. They also follow paper-based activities of each lesson where possible and appropriate.

Monitoring and Review

All actions in the ICT Development plan have identified staff responsible, associated performance indicators, target dates and suggested evidence for completion. The sections of the plans are reviewed monthly by the ICT Co-ordinator and link Leadership Team member during line management meetings. A formal review of progress occurs annually.

Learning Out of College Hours

Support and access to computers is necessary for all students to complete their coursework outside lesson times . An ICT suite is available during lunch break every day to facilitate this access and is supervised by a member of the ICT Support Team.

It has always been evident that some students have a strong interest in ICT that can be nurtured outside lessons, through specialised clubs, courses, and online materials. ICT Support occasionally advertises for student technicians to assist the ICT technicians with general ICT support work for students from year 11 upwards.

Access to online courses is encouraged through the college website and Virtual Learning Environment (VLE).

Home - College links

The college website is intended to provide parents with information about the college (contacts, directions, term dates, lesson times, policies, canteen menus etc.) and to indicate to parents (and students) where they can find information and advice about examinations, revision, careers, bullying, drugs, etc.)

A Virtual Learning Environment (VLE) is set up so that students (and parents) can access learning materials provided by the college.

The Parent Portal is currently available to all parents giving assessment and profile data on their child as at set periods of time.

It is planned to facilitate online galleries to enable parents to view their child's work at college.

Legislation

The college takes its legal responsibilities very seriously, particularly compliance with software licensing. All licences, keys, and original disks are stored in ICT Support.

Students are prevented from downloading music, video, or program files to prevent abuse of copyright. This is reinforced throughout the ICT scheme of work.

Staff with access to student data are instructed about data protection during the induction process and reminded of the reasons why passwords need to be secure several times a year.

All regular users or computers are monitored under the Display Screen Equipment (DSE) regulations. An annual assessment is carried out by the ICT Systems Manager and appropriate changes made, in accordance with the guidelines of the local authority.

The efficient running of the network and email facilities

The Information Access and Security policy describes the actions and responsibilities required for the secure, resilient, and efficient running of the college network, including backups, archiving, access permissions, and antivirus precautions.

Staff are warned about the dangers and protocols of using email.

Appendices

1. E-Safety Policy
2. Acceptable Use of ICT for Staff Working In The College
3. Acceptable Use of Computers and the Internet by Students
4. Uplands Community College Guidelines to Inappropriate Internet Access
5. Internet Safety Check Sheet For teachers
6. Student Internet Use Agreement
7. Guidelines For Teachers In ICT Rooms
8. Staff Laptop Use Policy
9. Guidelines for Developing College Websites
10. Acceptable Use Of Email Policy
11. Summary guidance for Parents
12. Social Media Policy

Appendix 1 - E-Safety Policy

E-Safety encompasses Internet technologies and electronic communications such as mobile phones and wireless technology. It highlights the need to educate children and young people about the benefits and risks of using new technology and provides safeguards and awareness for users to enable them to control their online experiences.

The college's E-Safety Policy will operate in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection, and Security.

Good Practice

E-Safety depends on effective practice at a number of levels:

- Responsible ICT use by all staff and students; encouraged by education and made explicit through published policies;
- Sound implementation of E-Safety policy in both administration and curriculum, including secure college network design and use;
- Safe and secure broadband including the effective management of content filtering;
- National Education Network standards and specifications.

The college will appoint an E-Safety group. This will be the Designated Child Protection Officer, a member of the Leadership Team, Health and Safety Co-ordinator and the ICT Systems Manager.

Our E-Safety Policy has been written by the college. It will be agreed by the Leadership Team and will be approved by governors.

The E-Safety Policy will be reviewed annually. This policy will next be reviewed in July 2017.

Why is Internet use important?

The purpose of Internet use in the college is to raise educational standards, to promote student achievement, to support the professional work of staff and to enhance the college's management information and administration systems.

Internet use is part of the statutory curriculum and a necessary tool for learning. It is an essential element in 21st century life for education, business, and social interaction. Access to the Internet is therefore an entitlement for students who show a responsible and mature approach to its use. Our college has a duty to provide students with quality Internet access.

Students will use the Internet and VLE outside college and will need to learn how to evaluate Internet information and to take care of their own safety and security.

How does Internet use benefit education?

Benefits of using the Internet in education include:

- Access to learning wherever and whenever convenient;
- Access to world-wide educational resources including museums and art galleries;
- Educational and cultural exchanges between students world-wide;
- Access to experts in many fields for students and staff;
- Professional development for staff through access to national developments, educational materials and effective curriculum practice;
- Collaboration across support services and professional associations;
- Improved access to technical support including remote management of networks and automatic system updates;
- Exchange of curriculum and administration data with the Local Authority and DCSF.

How can Internet use enhance learning?

- The college Internet access will be designed expressly for student use and includes filtering appropriate to the age of students;
- Students will be taught what Internet use is acceptable and what is not and given clear objectives for Internet use;
- Internet access will be planned to enrich and extend learning activities;
- Staff should guide students in on-line activities that will support learning outcomes planned for the students' age and maturity;
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation;
- Students will be educated in the effective use of the VLE.

Authorised Internet access

- All staff must read and sign the 'Acceptable ICT Use Agreement' before using any college ICT resource;
- Parents will be informed that students will be provided with supervised Internet access;
- Parents will be asked to sign and return a consent form for student access;
- Students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement.

World Wide Web

- If staff or students discover unsuitable sites, the URL (address), time, content must be reported to the E-Safety policy group, ICT Systems Manager or Deputy Head for ICT Strategy;
- Uplands Community College will ensure that the use of Internet derived materials by students and staff complies with copyright law;
- Students will be taught to be critically aware of the materials they are shown and how to validate information before accepting its accuracy through Key Stage 3 and Key Stage 4 programmes of study.

Email

- Students may only use approved e-mail accounts on the college system;
- Students must immediately tell a teacher if they receive offensive email;
- Students must not reveal personal details of themselves or others in e-mail communication, or arrange to meet anyone without specific permission;
- Access in college to external personal email accounts may be blocked;
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on college headed paper;
- The forwarding of chain letters is not permitted.

Social networking

- The college will block/filter access to social networking sites and newsgroups unless a specific use is approved;
- Students will be advised never to give out personal details of any kind which may identify them or their location;
- Students should be advised not to place personal photos on any social network space;
- Students should be advised on security and encouraged to set passwords, deny access to unknown individuals, and instructed how to block unwanted communications. Students should be encouraged to invite known friends only and deny access to others.

Filtering

The college will work in partnership with the Local Authority and MSP to ensure filtering systems are as effective as possible.

Video conferencing

- IP video conferencing should use the educational broadband network to ensure quality of service and security rather than the Internet;
- Students should ask permission from the supervising teacher before making or answering a videoconference call;
- Video conferencing will be appropriately supervised for the students' age.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in college is allowed;
- Mobile phones will not be used for personal use during lessons or formal college time. The sending of abusive or inappropriate text messages is forbidden;
- Keep Kids Safe is the chosen method of SMS contact with parents and students.

Published content and the college website

- The contact details on the website will be the college address, email and telephone number. Staff or students personal information will not be published;
- The Headteacher will take overall editorial responsibility and ensure that content is accurate and appropriate.

Publishing students' images and work

- Photographs that include students will be selected carefully and will be appropriate for the context;
- Students' full names will not be used anywhere on the website in association with photographs;
- Written permission from parents or carers will be obtained annually before photographs of students are published on the college website.

Information system security

- College ICT systems capacity and security will be reviewed regularly;
- Virus protection will be installed and updated daily;
- Security strategies will be discussed with the Local Authority.

Protecting personal data

Personal data will be recorded, processed, transferred, and made available according to the Data Protection Act 1998.

Assessing Risks

The college will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked Internet content, it is not possible to guarantee that unsuitable material will never appear on a college computer. Neither the college nor East Sussex Council can accept liability for the material accessed, or any consequences of Internet access. The college will audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate.

Handling E-Safety complaints

- A senior member of staff will deal with complaints of Internet misuse;
- Any complaint about staff misuse must be referred to the Headteacher;
- Complaints of a child protection nature must be dealt with in accordance with college child protection procedures;
- Students and parents will be informed of the complaints procedure.

Communication of policy

Students

- Rules for Internet access will be posted in all classrooms;
- Students will be informed that Internet use will be monitored.

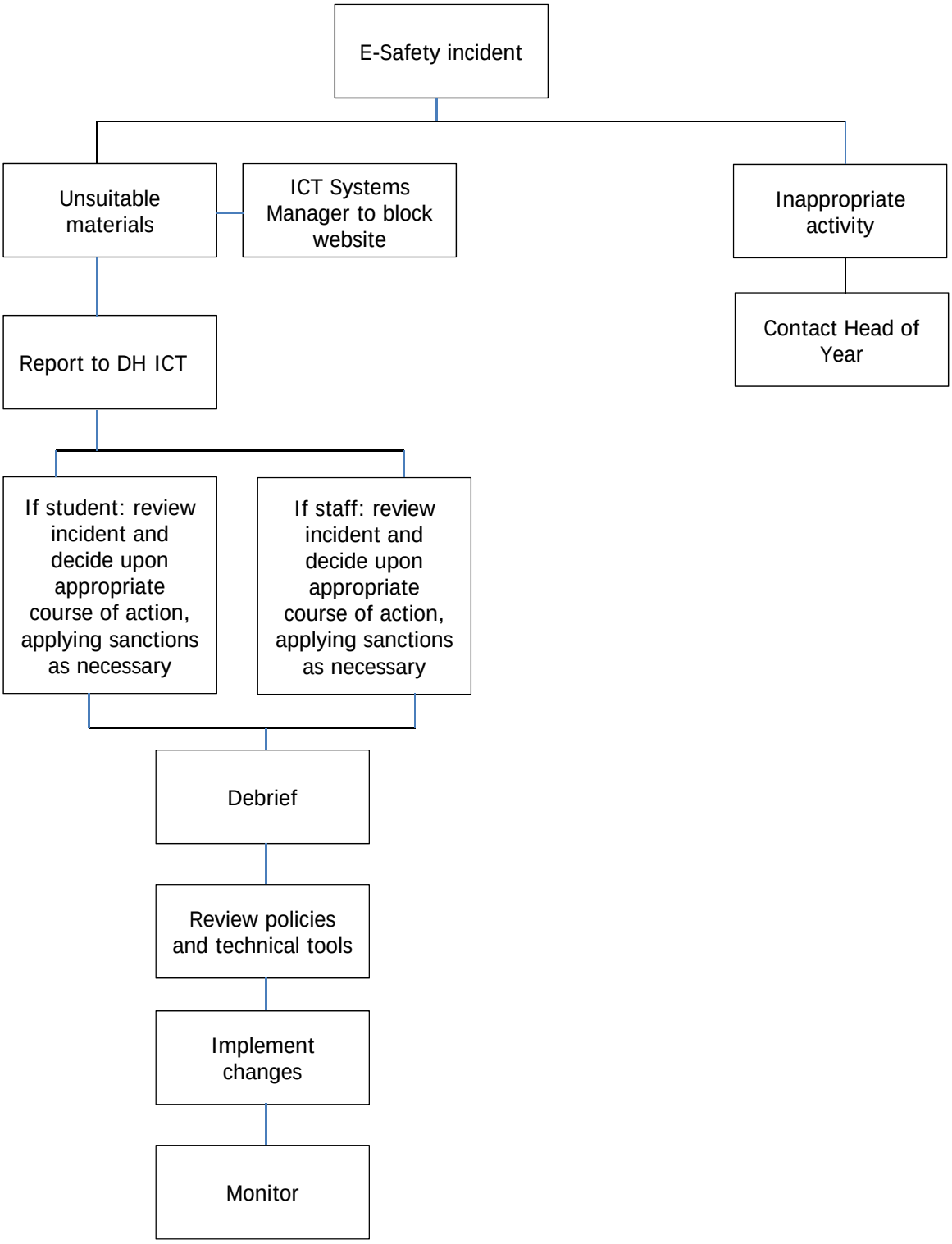
Staff

- All staff will be given the college E-Safety Policy and its importance explained;
- Staff should be aware that Internet traffic could be monitored and traced to the individual user. Discretion and professional conduct is essential;
- Staff that manage filtering systems or monitor ICT use will be supervised by senior management and have clear procedures for reporting issues.

Parents

Parents' attention will be drawn to the college E-Safety Policy in newsletters, the college brochure and on the college Web site and VLE.

Flowchart for responding to E-Safety incidents in college



Adapted from Becta – E-Safety 2005

E-Safety Rules

These E-Safety rules help to protect students and the college by describing acceptable and unacceptable computer use.

- The college owns the computer network and can set rules for its use;
- It is a criminal offence to use a computer or network for a purpose not permitted by the college;
- Irresponsible use may result in the loss of network or Internet access;
- Network access must be made via the user's authorised account and password, which must not be given to any other person;
- All network, memory sticks, and Internet use must be appropriate to education;
- Copyright and intellectual property rights must be respected;
- Messages shall be written carefully and politely, particularly as email could be forwarded to unintended readers;
- Anonymous messages and chain letters are not permitted;
- Users must take care not to reveal personal information through email, personal publishing, blogs, or messaging;
- The college ICT systems may not be used for private purposes, unless the Principal has given specific permission;
- Use for personal financial gain, gambling, political activity, advertising or illegal purposes is not permitted.

The college will exercise its right to monitor the use of the college's computer systems, including access to websites, the interception of email and the deletion of inappropriate materials, where it believes unauthorised use of the college's computer system may be taking place, or the system may be being used for criminal purposes, or for storing unauthorised or unlawful text, imagery or sound.

Uplands Community College
E-Safety Rules

All students use computer facilities including Internet access as an essential part of learning, as required by the National Curriculum. Both students and their parents/carers are asked to sign to show that the E-Safety Rules have been understood and agreed.

Student:	**Form:**

Students' Agreement

- I have read and I understand the college E-Safety Rules;
- I will use the computer, network, mobile phones, Internet access and other new technologies in a responsible way at all times;
- I know that network and Internet access may be monitored.

Signed:	**Date:**

Parent's consent for web publication of work and photographs

I agree that my son/daughter's work may be electronically published. I also agree that appropriate images and video that include my son/daughter may be published subject to the college rule that photographs will not be accompanied by pupil names.

Parent's consent for Internet access

I have read and understood the college E-Safety rules and give permission for my son / daughter to access the Internet. I understand that the college will take all reasonable precautions to ensure that students cannot access inappropriate materials but I appreciate that this is a difficult task.

I understand that the college cannot be held responsible for the content of materials accessed through the Internet. I agree that the college is not liable for any damages arising from use of the Internet facilities.

Signed:	**Date:**

Please print name:

Please complete, sign and return to the college

Staff Information Systems Code of Conduct

To ensure that staff are fully aware of their professional responsibilities when using information systems, they are asked to sign this code of conduct. Staff should consult the college's E-Safety policy for further information and clarification.

- The information systems are college property and I understand that it is a criminal offence to use a computer for a purpose not permitted by its owner;
- I will ensure that my information systems use will always be compatible with my professional role;
- I understand that college information systems may not be used for private purposes, without specific permission from the Headteacher;
- I understand that the college may monitor my information systems and Internet use to ensure policy compliance;
- I will respect system security and I will not disclose any password or security information to anyone other than an appropriate system manager;
- I will not install any software or hardware without permission;
- I will ensure that personal data is kept secure and is used appropriately, whether in college, taken off the college premises or accessed remotely;
- I will respect copyright and intellectual property rights;
- I will report any incidents of concern regarding children's safety to the college E-Safety Coordinator or the Designated Child Protection Coordinator;
- I will ensure that any electronic communications with students are compatible with my professional role;
- I will promote E-Safety with students in my care and will help them to develop a responsible attitude to system use and to the content they access or create.

The college may exercise its right to monitor the use of the college's information systems, including Internet access, the interception of email and the deletion of inappropriate materials where it believes unauthorised use of the college's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

I have read, understood and agree with the Information Systems Code of Conduct.

Signed: …….. Name: …….. Date: ……

E-Safety Audit – Secondary Colleges

This quick self-audit will help the senior leadership team (SLT) assess whether the E-Safety basics are in place.

Has the college an E-Safety Policy that complies with CYPD guidance?	Y/N
Date of latest update:	
The Policy was agreed by governors on:	
The Policy is available for staff at:	
And for parents at:	
The designated Child Protection Teacher/Officer is:	
The E-Safety Coordinator is:	
Has E-Safety training been provided for both students and staff?	Y/N
Is the Think U Know training being considered?	Y/N
Do all staff sign an ICT Code of Conduct on appointment?	Y/N
Do parents sign and return an agreement that their child will comply with the College E-Safety Rules?	Y/N
Have college E-Safety rules been set for students?	Y/N
Are these rules displayed in all rooms with computers?	Y/N
Is Internet access provided by an approved educational Internet service provider and complies with DCSF requirements for safe and secure access?	Y/N
Has the college filtering policy been approved by the Leadership Team?	Y/N
Is personal data collected, stored and used according to the principles of the Data Protection Act?	Y/N
Are staff with responsibility for managing filtering, network access and monitoring adequately supervised by a member of the Leadership Team?	Y/N

Appendix 2 - Uplands Community College acceptable use of ICT for staff

Uplands Community College has provided computers for use by staff, offering access to a vast amount of information for use in studies, acting like an enormous extension to the school library and offering great potential to support the curriculum.

The computers are provided and maintained for the benefit of all staff, and you are encouraged to use and enjoy these resources, and help to ensure they remain available to all. Remember that access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Equipment

- Always get permission before installing, attempting to install or storing programs of any type on the computers;
- Damaging, disabling, or otherwise harming the operation of computers, or intentionally wasting resources puts your work at risk, and will cut short your time with the ICT equipment;
- Only use the computers for educational purposes. Activities such as buying or selling goods are inappropriate;
- Always check files brought in on removable media (such as floppy disks, CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses;
- Always check mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) with antivirus software and ensure they have been found to be clean of viruses before connecting them to the network;
- Protect the computers from spillages by eating or drinking well away from the ICT equipment.

Security and privacy

- Protect your work by keeping your password to yourself; never use someone else's logon name or password;
- Always be wary about revealing your home address, telephone number, school name, or picture to people you meet on the Internet;
- Other computer users should be respected and should not be harassed, harmed, offended or insulted;
- To protect yourself and the systems, you should respect the security on the computers; attempting to bypass or alter the settings may put you or your work at risk;
- Computer storage areas and floppy disks will be treated like school lockers. ICT staff may review your files and communications to ensure that you are using the system responsibly.

Internet

- You should access the Internet only for school activities;
- Only access suitable material; using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted;
- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws;
- 'Chat' activities take up valuable resources which could be used by others to benefit their studies, and you can never be sure who you are really talking to. For these reasons 'chat' rooms should be avoided.

Email

- Be polite and appreciate that other users might have different views from your own. The use of strong language, swearing or aggressive behaviour is as anti-social on the Internet as it is on the street;
- Only open attachments to emails if they come from someone you already know and trust. Attachments can contain viruses or other programs that could destroy all the files and software on your computer;
- If you receive an email containing material of a violent, dangerous, racist, or inappropriate content, always report such messages to a member of ICT staff. The sending or receiving of an email containing content likely to be unsuitable for schools is strictly forbidden.

Please read this document carefully. Once it has been signed and returned will access to the Internet be permitted. If you violate these provisions, access to the Internet could be denied and you could be subject to disciplinary action. Additional action may also be taken by the school in line with existing policy regarding staff behaviour. Where appropriate, police may be involved or other legal action taken.

Appendix 3 - acceptable use of computers and the Internet by students

The college has purchased and installed computers, with an Internet connection, to enhance the facilities for learning. Students must agree to use the computers responsibly and to avoid the dangers of the Internet.

- Students must only access computer systems with their own username and password, which they should keep secret;
- Students must not try to access other people's files;
- Students must not try to bypass any of the security systems that are in use;
- Students must only use the college computers for college work and homework;
- Students must avoid websites or files containing inappropriate material (e.g. violence, racism, pornography) and report any such material immediately, to a member of staff;
- Students must only email people they know, or their teachers have approved;
- The messages students send should be polite and responsible;
- Students must not give their home address or telephone number, or arrange to meet someone, unless their parent, guardian or teacher has given permission;
- Students must report any unpleasant material or messages sent to them;
- Students must not interfere with any equipment or connections;
- Students must report any failure of, or damage to, computer equipment as soon as they notice it;
- Students must respect copyright;
- Students must not install any files on college computers without the permission of a teacher;
- The college will check computer files and monitor the internet sites students' visit.

Appendix 4 - Uplands Community College guidelines to inappropriate Internet access

Whilst using the Internet during college hours, a student deliberately types in a website address that will display inappropriate material. What should you do?

Use this step-by-step guide to help you follow the correct procedure for dealing with students deliberately searching for inappropriate materials on the Internet.

- Explain to the student that they have broken the rules of the college's Acceptable User Policy (AUP) and Internet Code of Conduct and that their behaviour is unacceptable;
- Take the student off the computer for the duration of the lesson. At a convenient time, ask the student to explain what happened and tell them that by doing so they may lessen the seriousness of the incident;
- Draw the student's attention to the Internet Code of Conduct that they agreed with their parents on starting at the college, which is summarized on the poster displayed in your ICT area;
- Discuss the incident with the Deputy Head ICT who will make a decision whether to write home to parents;
- Report the incident to the ICT Systems Manager, so that the college filtering system can be improved accordingly.

Sanctions

- The sanctions are as per the college behaviour policy for breaking rules (e.g. removing the student's Internet access for a period of time, informing the student's parents);
- Sanctions will vary as to the inappropriateness of the material accessed;
- In all cases, the teacher involved must set detentions. Other detentions will be set as required by the Deputy Head of ICT and/or the Head of Year.

Appendix 5 - Internet safety check sheet for teachers

It is good practice to discuss these points with students at the start of the college year, the start of a project requiring internet use, or if revision of acceptable internet use is necessary.

Remind students to:

- Only use the Internet when there is a teacher or other adult present to supervise or when you have been given specific permission.
- Only use your own login name and password.
- Never give out your address, phone number or arrange to meet someone over the Internet.
- All e-mails should be polite, appropriate, and sensible.
- If you receive a rude or offensive message or if you feel uncomfortable about anything, you must report it to a teacher immediately.
- Be aware that the college may check your computer files and monitor the Internet sites you visit.
- Ask an adult if you are unsure that a web source is reliable and information you are going to use is accurate.
- You and your parents should have signed the college Internet agreement. You will be breaking that agreement if you deliberately break these rules. This could result in you losing your Internet access at college.

Draw student's attention to the poster on the wall in the suite/classroom regarding sensible conduct whilst using the Internet. They can refer to this anytime they need a reminder.

Appendix 6 - student Internet use agreement

Student:……. **Tutor Group**:…….

Date:…….

My parents and I have read the Code of Conduct for Internet Use and I agree to follow it.

Student signature:…… **Date**:……

Parent

As parent or guardian, I have read, discussed, and explained the Code of Conduct for Internet use to my son/daughter. I understand that if he/she fails to follow this code, his/her individual access will be withdrawn and I will be informed.

Parent/guardian signature:……. **Date**:…….

Permission and copyright release

This college may produce printed publications and/or a college website which may include examples of pupil's work and/or photographs of students. No child's work will ever be used without his/her permission and we take the issue of child safety very seriously, which includes the use of images of students. Including images of students in college publications and on the college website can be motivating for the students involved, and provide a good opportunity to promote the work of the college. However, colleges have a duty of care towards students, which means that students must remain unidentifiable, reducing the risk of inappropriate contact, if images are used in this way.

We ask that parents' consent to the college publishing their children's work and to the taking and using of photographs and images of their children subject to strict confidentiality of personal information. (This can be changed at any time; contact the Headteacher or Deputy Head ICT).

I consent to photographs and digital images of the child named above, appearing in printed publications or on the college website. I understand that the images will be used only for educational purposes and that the identity of my child will be protected. I also acknowledge that the images may also be used in and distributed by other media, such as CD-ROM, as part of the promotional activities of the college. I also consent to examples of my child's work being published on the college website or in other media, subject to strict confidentiality of personal information.

Parent/guardian signature :……. **Date** :…….

Appendix 7 - guidelines for teachers in ICT rooms

Start of the lesson – entering the room
Students should know not to enter an ICT room without a teacher telling them. Students should be instructed to enter the classroom in a calm and orderly manner four or five at a time and should follow your seating plan or sit in the nearest available seat.

Start of the lesson - checking
Students should check their computer at the start of their lesson. If anything is missing or broken, they should let you know. You can remind them that they are now responsible for the computer they use until the end of the lesson. This means they should watch over it at all times.

If there is a fault or a missing or broken component, you should contact ICT Support.

Start of the lesson – cables and connections
Under no circumstances should anyone except a technician touch the back of the computers including cables and connections. The same applies to computer screens and sockets at the front of the PC. There should be no reason for a student to touch these unless they have permission to use a jump drive.

End of the lesson – allow time for tidying, checking and proper logging off
Students should log out properly at least three minutes before the end of the lesson. The keyboard and mouse should be left tidy and straight so the computer can be easily checked and any further problems reported. All paper, worksheets and litter should be removed from tables, floor and around the printer, Chairs should also be tucked under tables and students dismissed one row at a time.

Students are expected to shut down using the mouse and should not press reset buttons or mains switches unless there is something wrong. Even then, they should ask you first. At the end of a lesson, all they need to do is log out. Shutting down incorrectly can damage the configuration or even the hardware.

Throughout the lesson – smart boards and interactive white boards
Do not use ordinary board markers for this equipment. Only use the pens provided.

Throughout the lesson - printing
Students should not print without your permission. Students have a quota, which is refreshed every week. If they run out during the lesson, they should request an increase in their quota.

Throughout the lesson – no eating or drinking
Students - including sixth formers - are not allowed to eat or drink in computer rooms.

Throughout the lesson – no games
The college policy is not to allow computer games in lesson time unless authorised by the teacher. Please make a note of games sites that are not already banned and report to ICT Support to add to the blacklist.

Throughout the lesson – use of internet
If you see a student accessing inappropriate material on the Internet, the Deputy Head of ICT should be notified. If you suspect a student but have no proof, please ask the ICT Support Manager to investigate giving details about which computer and when it happened.

Further support
Please remember if you are using an ICT teacher's main teaching room. That teacher, time permitting, could well be willing to reinforce your instructions to the class or to remind you of particular issues in their room.

Delivery of Lessons in an ICT Room

When delivering lessons using ICT you will find that the best quality work will come out of following these simple guidelines.

1. Always ensure that students save work regularly into the appropriate folders;
2. Always remind students of appropriate use and the sanctions if this is not followed;
3. Always ensure that your objectives are on the board;
4. Always ensure that you give students a sense of audience and purpose;
5. Always demonstrate an example of what you expect them to deliver;
6. Always demonstrate the basic steps of the software as a reminder;
7. The SMART Skills books in ICT rooms can provide students with additional help with specific skills; they are familiar with these books so encourage them to use them in your lessons;
8. Before applying any formatting, have students plan and gather the content;
9. Use planning templates on paper before the ICT lesson. This will allow them to think about and focus on the ICT during the lesson;
10. You could follow the project life cycle of:
    a. Identify – purpose and audience of the task. Create a Gantt chart of how long they have to complete and when they will do each task;
    b. Analyse – what do I need in terms of software and other resources? What exactly must my information do?
    c. Design – use paper planning if necessary or open mind to plan the task, choose appropriate software;
    d. Implementation – carry out research, put into appropriate software;
    e. Test – peer and self-evaluation, teacher evaluation - against the task criteria;
    f. Improve – update with feedback (always save two versions, before and after);
    g. Evaluation – what did we do, how did we do it? How could we improve if we did it again?

Appendix 8 - Uplands Community College staff laptop policy

Risk:

- Laptops being used mainly at home;
- Virus definition updates connecting to home networks, and use by non-college personnel;
- Non-secured networks in the home.

Target group:

- All college staff who take college laptops home.

Effect:

- Computers are open to attack unless virus definitions are updated regularly. Spyware can transmit data from the laptop back to unknown sources;
- Use of college property by non-college personnel breaches Acceptable Use policies, and may give rise to unacceptable material being stored in the device;
- Authorised users not being aware that use of the equipment by non-college employees is not permitted;
- Unauthorised access to the laptop through unencrypted wireless networks.

Detection:

- Laptops failing owing to security breaches;
- Laptops becoming infected and attempting to pass on infection to college networks;
- Unacceptable material being found on hard drives.

Recommended Countermeasure:

- All college laptops must be brought into college once a week and connected to the college domain for virus definition updates;
- A clear statement in Acceptable Use policies that college equipment must only be used by college personnel. If the device is to be connected to an external wireless network, that network must be properly encrypted. (WEP 64 bit as a minimum, with WPA being preferred);
- Staff must password lock the laptop whilst in use to ensure there is no unauthorised access.

Links with Policies:

- Staff taking college equipment home must ensure that it is not used by non-college staff. All staff using college laptops at home for periods of longer than one week must bring them into college and connect to the domain in order for the virus definition files to be updated;
- The user must ensure that all wireless networks to which this equipment is to be connected must be securely encrypted;
- Staff are not permitted to install software that does not comply with the relevant licensing;
- Accidental damage or theft must be covered by their home insurance.

Appendix 9 - Guidelines for developing college websites

Adapted from the Superhighway Safety web site http://www.safety.ngfl.gov.uk/

The use of photographs of students

- Avoid the use of the first name and surname of individuals in a photograph. This reduces the risk of inappropriate, unsolicited attention from people outside the college;
- Ensure that the information you send to parents concerning their child's use of the internet includes a statement indicating that you may use students' photographs on the college web site but that children will not be named on such photographs. This ensures that parents are aware of the way the image of their child is representing the college;
- Use photographs of items designed and made in technology lessons, excerpts from written work and scanned images of artwork. This allows students to exhibit their work to a wider audience without increasing the risk of inappropriate use of images of students. As with photographs of students, make sure that parents are aware that you may use photographs of students' work on the college web site;
- Only use images of students in suitable dress to reduce the risk of inappropriate use;
- Create a recognised procedure for reporting the use of inappropriate images to reduce the risks to students.

Background

Including images of students on the college website can be motivating for the students involved and provide a good opportunity to promote the work of the college. It is important to balance the potential risks of including images of students on the website against the design principles of creating colourful, attractive, and relevant pages, as the college, Headteacher and governors would do with any publication.

Colleges need to develop a policy in relation to the use of images of students on the college website. The Headteacher and governors will need to make decisions about the type of images they consider suitable and that appropriately represent the college. They will want to ensure parents support their policy. When assessing the potential risks in the use of images of students, the most important factor is the potential of inappropriate use of images of children.

Providing the name and photograph of a student on a website allows for the possibility of people outside of the college identifying and then contacting students directly. Avoiding the use of images of named individuals therefore reduces the risk of unsolicited attention.

Colleges may want to include images of an individual or a group of children who have won a competition or took part in a college trip. Avoiding naming students who feature in the image reduces the risk of inappropriate contact.

Appendix 10 - acceptable use of email policy

Overview

This paper is a guideline for the acceptable use of email by the staff and students at Uplands Community College. This policy will be made available to all users of email and related services within the college. There will also be a periodic review of the Policy and, if necessary, amendments from time to time. This will be necessary with regard to the expected development of the system, the operational use of the system and generally recognised best practice. Email services are provided by the college to support its primary role of education and associated functions related to this role.

Statement of Authority

This policy is intended to detail the rules of conduct for all staff and students who use email and related services. This Email Policy applies to the use, for the purpose of sending or receiving email messages and attachments, of any IT facilities, including hardware, software and networks, provided by the college. The Policy is applicable to all members of the college including staff, students and other authorised users of college IT facilities.

Statement of Responsibilities

Individual users are responsible for their own actions. The use of email facilities by individuals at Uplands Community College assumes and implies compliance with this policy, without exception. Every user of email systems has a duty to ensure they practice appropriate and proper use and must understand their responsibilities in this regard.

Acceptable Use

- The college's main purpose in providing IT facilities for email is to support the teaching, learning, research and approved business activities of the college. IT facilities provided by the college for email should not be abused. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to):
- Creation or transmission of material which brings the college into disrepute;
- Creation or transmission of material that is illegal;
- The transmission of unsolicited commercial or advertising material, chain letters, press releases or other junk mail of any kind;
- The unauthorised transmission to a third party of confidential material concerning the activities of the college; The transmission of material such that this infringes the copyright of another person, including intellectual property rights;
- Activities that unreasonably waste staff effort or networked resources, or activities that unreasonably serves to deny service to other users.

Please note this includes sensitive and sensible use of the ‘cc’ option when distributing emails – avoid copying in large groups of individuals.

- Activities that corrupt or destroy other users' data or disrupt the work of other users;
- Unreasonable or excessive personal use;
- Creation or transmission of any offensive, obscene or indecent images, data or other material;
- Creation or transmission of material which is designed or likely to cause annoyance, inconvenience or anxiety;
- Creation or transmission of material that is abusive or threatening to others, serves to harass or bully others, discriminates or encourages discrimination on racial or ethnic grounds, or on grounds of gender, sexual orientation, marital status, disability, political or religious beliefs;
- Creation or transmission of defamatory material or material that includes claims of a deceptive nature;
- Activities that violate the privacy of others or unfairly criticise, misrepresent others; this includes copying distribution to other individuals;
- Creation or transmission of anonymous messages or deliberately forging messages (i.e., without clear identification of the sender) or for 'flaming'.

Personal use
The college permits the use of its IT facilities for email by students, staff, and other authorised users for a reasonable level of personal use. An absolute definition of abuse is difficult to achieve but certainly includes (but is not necessarily limited to) a level of use that is not detrimental to the main purpose for which the facilities are provided. Priority must be given to use of resources for the main purpose for which they are provided.

- Not being of a commercial or profit-making nature, or for any other form of personal financial gain;
- Not be of a nature that competes with the college in business;
- Not be connected with any use or application that conflicts with an employee's obligations to the college as their employer;
- Not be against the college's rules, regulations, policies, and procedures and in particular this email policy.

Incident handling
The college will investigate complaints from both internal and external sources. If there is evidence of an offence, it will be investigated in accordance with college regulations and procedures. Email and network accounts could be suspended or stopped and if the offence warrants it, external agencies such as the Police or East Sussex County Council will be contacted.

Maintenance and Storage
Individual users should be aware that the college has a finite capacity for the storage of emails on its servers. It is therefore essential that individual users' act responsibly in keeping the volume of email stored in their 'inbox' and other email folders to a minimum. There are number of practical steps individual users can take to maintain their email folders responsibly. These include:

- Deleting read emails from one's **'Inbox'** that do not contain any information that needs to be filed away for future reference e.g. acknowledgements, arranging meeting times etc.;
- Regularly deleting items in one's '**Sent Items'** folder that do not contain any information that needs to be filed away for future reference e.g. acknowledgements, arranging meeting times etc.;
- Setting up your email account to empty your **'Deleted Items'** folder on when logging out of email;
- Conducting a regular (termly) review of all email folders to delete stored items that are no longer required;
- Sensible and sensitive use of the **'cc'** option when transmitting emails. Large distribution lists put a strain on the college's network and storage capacity.

The college regularly monitors its email storage capacity. Please note if levels of email storage start to reach unacceptable levels the ICT Systems Manager will identify and contact those individual users who have stored too much email.

In this instance, the individual will be required to take immediate action to reduce the volume of email stored in their account **within one week** of the initial contact.

If no action results the ICT Systems Manager reserves the right to freeze the individual users account until the necessary action is taken and in addition the ICT Systems Manager will implement a storage capacity limit on the individual user's account to ensure the situation does not arise again in future.

Appendix 11 - social media policy

Introduction

- The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*;
- While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Uplands Community College staff and contractors are expected to follow when using social media;
- It is crucial that pupils, parents and the public at large have confidence in the school's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of the school and East Sussex County Council are safeguarded;
- Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

Scope

- This policy applies to Uplands Community College governing body, all teaching and other staff, whether employed by the County Council or employed directly by the school, external contractors providing services on behalf of the school or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the school. These individuals are collectively referred to as 'staff members' in this policy;
- This policy covers personal use of social media as well as the use of social media for official school purposes; including sites hosted and maintained on behalf of the school (see sections 5, 6, 7 and Appendices A and B);
- This policy applies to personal webspace such as social networking sites (for example *Facebook*, *MySpace*), blogs, mircoblogs such as *Twitter*, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

Legal framework

- Uplands Community College is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the school are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:
    - The Human Rights Act 1998;
    - Common law duty of confidentiality, and
    - The Data Protection Act 1998.
- Confidential information includes, but is not limited to:
    - Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998;
    - Information divulged in the expectation of confidentiality;
    - School or County Council business or corporate records containing organisationally or publicly sensitive information;
    - Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
    - Politically sensitive information.

- Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:
    - Libel Act 1843;
    - Defamation Acts 1952 and 1996;
    - Protection from Harassment Act 1997;
    - Criminal Justice and Public Order Act 1994;
    - Malicious Communications Act 1998;
    - Communications Act 2003, and
    - Copyright, Designs and Patents Act 1988.
- Uplands Community College and the County Council could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online, or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc. or who defame a third party while at work may render Uplands Community College or the County Council liable to the injured party.

Related policies

- This policy should be read in conjunction with the following school and County Council policies:
    - East Sussex County Council Code of Conduct for Employees;
    - Uplands Community College ICT Policy;
    - Staff Acceptable Use Policy.

Principles – be professional, responsible and respectful

- You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the school or County Council and your personal interests.
- You must not engage in activities involving social media that might bring Uplands Community College or the County Council into disrepute.
- You must not represent your personal views as those of Uplands Community College or the County Council on any social medium.
- You must not discuss personal information about pupils, Uplands Community College or County Council staff, and other professionals you interact with as part of your job on social media.
- You must not use social media and the internet in any way to attack, insult, and abuse or defame pupils, their family members, colleagues, other professionals, and other organisations, Uplands Community College or the County Council.
- You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Uplands community College or the County Council.

Personal use of social media

- Staff members must not identify themselves as employees of Uplands Community College or County Council or service providers for the school or County Council in their personal webspace. This is to prevent information on these sites from being linked with the school and the County Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services;
- Staff members must not have contact through any personal social medium with any pupil, whether from Uplands Community College or any other school, unless the pupils are family members;
- Uplands Community College does not expect staff members to discontinue contact with their family members via personal social media once the school starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way;
- Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity;

- If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the school and through official school sites created according to the requirements specified in section 7 and Appendix A;
- Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. Instead, if they receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official school site;
- On leaving Uplands Community College service, staff members must not contact Uplands Community College pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former schools by means of personal social media;
- Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues, County Council staff and other parties and school or County Council corporate information must not be discussed on their personal web space;
- Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school or County Council uniforms or clothing with school or County Council logos or images identifying sensitive school or County Council premises (e.g. care homes, secure units) must not be published on personal webspace;
- School or County Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media;
- Staff members must not edit open access online encyclopaedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself;
- Uplands Community College or County Council corporate, service or team logos or brands must not be used or published on personal web space;
- Uplands Community College does not allow access to social media for personal reasons while at work.
- Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place;
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often, and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

Using social media on behalf of Uplands Community College

- Staff members can only use official school sites for communicating with pupils or to enable students to communicate with one another;
- There must be a strong pedagogical or business reason for creating official school sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the school to unwelcome publicity or cause reputational damage;
- Official school sites must be created only according to the requirements specified in Appendix A of this policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements;
- Staff members must at all times act in the best interests of children and young people when creating, participating in, or contributing content to social media sites.

Monitoring of Internet use

- Uplands Community College monitors usage of its internet and email services without prior notification or authorisation from users;
- Users of Uplands Community College email and internet services should have no expectation of privacy in anything they create, store, send, or receive using the school's ICT system.

Breaches of the policy

- Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Uplands Community College or County Council Disciplinary Policy and Procedure;
- A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Uplands Community College or the County Council or any illegal acts or acts that render Uplands Community College or the County Council liable to third parties may result in disciplinary action or dismissal;
- Contracted providers of Uplands Community College or County Council services must inform the relevant school or County Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the school and the County Council. Any action against breaches should be according to contractors' internal disciplinary procedures.

Appendix 1 - requirements for creating social media sites on behalf of Uplands Community College

Creation of sites

- Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Uplands Community College;
- Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome;
- The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the school's Deputy Head of ICT Strategy;
- Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment;
- The Headteacher must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover;
- There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the school's brand and image;
- Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

Children and young people

- When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people;
- When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyber bullying;
- If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm;
- Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008);
- Staff members must also ensure that the web space they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site;
- Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted;
- Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the school or the County Council. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your Communications Manager (or appropriate manager);

Approval for creation of or participation in webspace

- Uplands Community College social media sites can be created only by or on behalf of the school. Site administrators and moderators must be Uplands Community College employees or other authorised people;
- Approval for creation of sites for work purposes, whether hosted by the college or hosted by a third party such as a social networking site, must be obtained from the staff member's line manager, the Deputy Head of ICT Strategy and Headteacher;
- Approval for participating, on behalf of Uplands Community College, on sites created by third parties must be obtained from the staff member's line manager, the Deputy Head of ICT Strategy and Headteacher;
- Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager, the Deputy Head of ICT Strategy and Headteacher;
- The Deputy Head of ICT Strategy must be consulted about the purpose of the proposed site and its content. In addition, the Headteacher's approval must be obtained for the use of the school logo and brand;
- Staff must complete the Social Media Site Creation Approval Form (Appendix B) and forward it to the Deputy Head of ICT Strategy before site creation;
- Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the Headteacher immediately. Staff members must not communicate with the media without the advice or approval of the Headteacher.

Content of webspace

- Uplands Community College hosted sites must have clearly expressed and publicised Terms of Use and House Rules. Third-party hosted sites used for work purposes must have Terms of Use and House Rules that conform to the school or County Council standards of professional conduct and service;
- Staff members must not disclose information, make commitments or engage in activities on behalf of Uplands Community College or the County Council without authorisation;
- Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the school's or County Council's image, reputation and services;
- Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment, and copyright law may apply to the content of social media.
- Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable;
- Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies;
- Uplands Community College hosted sites must always include the school logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the school website;
- Staff members participating in Uplands Community College hosted or other approved sites must identify who they are. They must disclose their positions within the school on these sites;
- Staff members must never give out their personal information such as home contact details or home email addresses on these sites;
- Personal opinions should not be expressed on official sites.

Contributors and moderation of content

- Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images;
- Sites created for and contributed to by students must have the strongest privacy settings to prevent breaches of confidentiality. Students and other participants in sites must not be able to be identified;
- The content and postings in Uplands Community College hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site;
- The team must designate at least two approved administrators whose role it is to review and moderate the content, including not posting or removal of comments, which breach the Terms of Use and House Rules. It is important that there are enough approved moderators to provide cover during leave and absences so that the site continues to be moderated;
- For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence;
- Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour;
- Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the College Policy must not be posted or removed. NOTE: The safer alternative is not to allow any outsiders to become friends of the site and to limit the site to known people only, in the case of adults, those who have undergone appropriate security checks;
- Any proposal to use social media to advertise for contributors to sites must be approved by the school's Headteacher;
- Approval must also be obtained from the school's Deputy Head of ICT Strategy to make an external organisation a 'friend' of the site.

Appendix 2 - social media site creation approval form

Use of social media on behalf of Uplands Community College must be approved prior to setting up sites.

Please complete this form and forward it to the school's Deputy Head of ICT Strategy.

TEAM DETAILS	
Department	
Name of author of site	
Author's line manager	
PURPOSE OF SETTING UP SOCIAL MEDIA SITE **(please describe why you want to set up this site and the content of the site)**	
What are the aims you propose to achieve by setting up this site? What is the proposed content of the site?	

PROPOSED AUDIENCE OF THE SITE
Please tick all that apply.

- ☐ Pupils of Uplands Community College
- ☐ Uplands Community College staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

PROPOSED CONTRIBUTORS TO THE SITE
Please tick all that apply.

- ☐ Pupils of Uplands Community College
- ☐ Uplands Community College staff
- ☐ Pupils' family members
- ☐ Pupils from other schools (provide names of schools)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

ADMINSTRATION OF THE SITE	
Names of administrators (the site must have at least 2 approved administrators)	
Names of moderators (the site must have at least 2 approved moderators)	

Who will vet external contributors?	
Who will host the site?	☐ Uplands Community College ☐ Third party; please give host name
Proposed date of going live	
Proposed date for site closure	
How do you propose to advertise for external contributors?	
If contributors include children or adults with learning disabilities, how do you propose to inform and obtain consent of parents or responsible adults?	
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' of the site?	

APPROVAL
(approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher).

Line Manager **I approve the aims and content of the proposed site.**	Name	
	Signature	
	Date	
Deputy Head ICT Strategy **I approve the aims and content of the proposed site.**	Name	
	Signature	
	Date	
Headteacher **I approve the aims and content of the proposed site and the use of school brand and logo.**	Name	
	Signature	
	Date	