E-Safety and Social Media Policy

<table>
<thead>
<tr>
<th>Document title</th>
<th>E-Safety and Social Media Policy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Policy number</td>
<td>S024</td>
</tr>
<tr>
<td>Version number</td>
<td>1.2</td>
</tr>
<tr>
<td>Policy status</td>
<td>Approved</td>
</tr>
<tr>
<td>Date of issue</td>
<td>August 2019</td>
</tr>
<tr>
<td>Date to be revised</td>
<td>August 2020</td>
</tr>
<tr>
<td>Owner</td>
<td>Carly Sargeant</td>
</tr>
<tr>
<td>Author</td>
<td>Carly Sargeant</td>
</tr>
</tbody>
</table>

Revision log (last 5 changes)

<table>
<thead>
<tr>
<th>Date</th>
<th>Version No</th>
<th>Brief detail of change</th>
</tr>
</thead>
<tbody>
<tr>
<td>27/06/18</td>
<td>1.1</td>
<td>A number of sections added and updated – Aims, Legislation and guidance, roles and responsibilities Cyber-Bullying, education and training, new staff training and others throughout</td>
</tr>
<tr>
<td>July 2019</td>
<td>1.2</td>
<td>Addition of Pastoral Manager’s role in monitoring Smoothwall and actioning interventions as a result. Addition of &quot;Education for a Connected World’ framework and a link to it in ‘Education’ section.</td>
</tr>
</tbody>
</table>
Contents

Aims 1
Legislation and guidance 1
The governing board 1
The Principal 2
The designated safeguarding lead 2
The ICT manager 2
All staff and volunteers 2
Parents 3
Visitors and members of the community 3
Some of the dangers young people may face include: 3
Scope of this policy 4
E-safety and anti-bullying 4
Cyber-bullying 4
Definition 4
Preventing and addressing cyber-bullying 4
Examining electronic devices 5
ICT Acceptable Use General Rules 5
Communicating E-Safety 6
Introducing the E-safety policy to students 6
Enlisting parents’ and carers support 6
E-safety Assemblies 6
Education and Training 7
Parents 7
Acceptable Usage Policy 8
Staff Training 8
Social Networking Sites 9
Monitoring 9
Incident Reporting 9
Responding to incidents of misuse 9
Training 10
Appendix 1 - Communications 11
Appendix 2 - Unsuitable / inappropriate activities 12
Appendix 3 14

Uplands Community College
E-Safety Rules 14
Staff Information Systems Code of Conduct 15
Social media policy
Introduction
Scope
Legal framework
Related policies
Principles – be professional, responsible and respectful
Personal use of social media
Using social media on behalf of Uplands Community College
Monitoring of Internet use
Breaches of the policy
Appendix 1 - requirements for creating social media sites on behalf of Uplands Community College
Creation of sites
Children and young people
Approval for creation of or participation in webspace
Content of webspace
Contributors and moderation of content
Appendix 2 - social media site creation approval form
E-Safety Audit – Secondary Colleges
Aims

New technologies have become integral to the lives of children and young people in today's society, both within the schools and in their lives outside school. The internet and other digital and information technologies are powerful tools, which open up new opportunities for everyone. Electronic communication helps teachers and students learn from each other. These technologies can stimulate discussion, promote creativity, and increase awareness of context to promote effective learning. The use of these exciting and innovative tools in school and at home has been shown to raise educational standards and promote student achievement. However, the use of these new technologies can put young people at risk within and outside the school.

Our College aims to:
- Have robust processes in place to ensure the online safety of pupils, staff, volunteers, and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole College community in its use of technology
- Establish clear mechanisms to identify, intervene, and escalate an incident, where appropriate

Legislation and guidance

This policy is based on the Department for Education’s statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department’s guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on pupils’ electronic devices where they believe there is a ‘good reason’ to do so.

The policy also takes into account the National Curriculum computing programmes of study.

Roles and responsibilities

The Governing Board

The Governing Board has overall responsibility for monitoring this policy and holding the Principal to account for its implementation.

The Governing Board will co-ordinate regular meetings with appropriate staff to discuss online safety, and monitor online safety logs as provided by the Designated Safeguarding Lead (DSL). The governor who oversees online safety is Jason Scott-Taggart.

All governors will:
- Ensure that they have read and understand this policy;
- Agree and adhere to the terms on acceptable use of the College’s ICT systems and the internet (Appendix 2).
The Principal

The Principal is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the College.

The Designated Safeguarding Lead

Details of the College’s designated safeguarding lead (DSL) [and deputy/deputies] are set out in our child protection and safeguarding policy.

The DSL takes lead responsibility for online safety in College, in particular:

- Supporting the Principal in ensuring that staff understand this policy and that it is being implemented consistently throughout the College;
- Working with the Principal, ICT Manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College behaviour policy;
- Updating and delivering staff training on online safety (Appendix 3 contains a self-audit for staff on online safety training needs);
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in College to the Principal and/or governing board.

This list is not intended to be exhaustive.

The ICT Manager

The ICT Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems (Smoothwall), which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at the College, including terrorist and extremist material, and communicating this to DSL team and Pastoral Manager;
- Ensuring that the College’s ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly;
- Conducting a full security check and monitoring the College’s ICT systems on a weekly basis;
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files;
- Ensuring that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy.

The Pastoral Manager

The pastoral manager is responsible for:

- Querying students in relation to blocked searches for harmful and inappropriate content;
- Communicating this to DSL, HOY and home and adding this to My Concerns;
- Putting appropriate interventions in place if the student needs further support;
- Referring student (e.g. Prevent, counselling, etc.) if the searches are significant/persistent;
This list is not intended to be exhaustive.

**All staff and volunteers**
All staff, including contractors and agency staff, and volunteers are responsible for:
- Maintaining an understanding of this policy;
- Implementing this policy consistently;
- Agreeing and adhering to the terms on acceptable use of the College’s ICT systems and the internet (Appendix 2), and ensuring that pupils follow the College’s terms on acceptable use (Appendix 1);
- Working with the DSL to ensure that any online safety incidents are logged (see Appendix 4) and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College behaviour policy.

This list is not intended to be exhaustive.

**Parents**
Parents are expected to:
- Notify a member of staff or the Principal of any concerns or queries regarding this policy;
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the College’s ICT systems and internet (Appendix 1).

Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? UK Safer Internet Centre: [https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues](https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues)

**Visitors and members of the community**
Visitors and members of the community who use the College’s ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use (Appendix 2).

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

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other College policies (e.g. behaviour, anti-bullying and child protection policies). As with all other risks, it is impossible to eliminate those risks completely. It is therefore essential, through good practice to build students’ resilience to the risks to which they may be exposed, so that they have the confidence and skills to face and deal with these risks.

The College provides the necessary safeguards to help ensure that we have done everything that could reasonably be expected to manage and reduce these risks. The e-safety policy explains how the College intends to do this, whilst also addressing wider educational issues in order to help young people (and their parents/carers/staff) to be responsible users and stay safe while using the Internet and other communications technologies for educational, personal, and recreational use.

**Scope of this policy**
This policy applies to all members of the College community (including staff, students, parents and carers, visitors, community users) who have access to and are users of the College’s ICT systems both in and out of College.

**E-safety and anti-bullying**
The e-safety policy has links with the Colleges anti-bullying policy since breaches of the e-safety policy could involve bullying of others.
(See the anti-bullying policy)

The impact of the policy will be monitored using:
- Incident logs;
- Internal monitoring using LanSchool software and Smoothwall;
- Feedback from survey and questionnaires issued to students, parents, and carers and staff.

**Cyber-bullying**

**Definition**
Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.
(See also the College behaviour policy.)

**Preventing and addressing cyber-bullying**
To help prevent cyber-bullying, we will ensure that pupils understand what it is and what to do if they become aware of it happening to them or others. We will ensure that pupils know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

The College will actively discuss cyber-bullying with pupils, explaining the reasons why it occurs, the forms it may take and what the consequences can be.
Form Tutors will discuss cyber-bullying with their tutor groups and the issue will be addressed in assemblies.

Teaching staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff, governors, and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support pupils, as part of safeguarding training (see section 11 for more detail).

The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it, and how they can support children who may be affected.

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

**Examining electronic devices**

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on pupils’ electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a ‘good reason’ to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or;
- Disrupt teaching, and/or;
- Break any of the College rules.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or;
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or;
- Report it to the police.

Any searching of pupils will be carried out in line with the DfE’s latest guidance on screening, searching and confiscation.

Any complaints about searching for or deleting inappropriate images or files on pupils’ electronic devices will be dealt with through the College complaints procedure.
ICT acceptable use general rules
Remember always treat others as you wish to be treated. The use of abusive, racist, homophobic or intolerant material is not allowed.

The following are not permitted:
- Sending, displaying, sharing or downloading offensive messages or pictures;
- Using obscene language;
- Posting malicious or false information about others;
- Harassing, insulting or attacking others;
- Damaging or attempting to damage computers, computer systems or computer networks;
- Violating copyright laws (e.g. downloading copyright protected music, videos or images etc.) without the express permission of the copyright holder;
- Using others passwords’ to gain access;
- Sharing of passwords to circumvent restrictions placed on other users;
- Intentionally wasting resources by others;
- Sending personally identifiable information to other online users without explicit permission;
- Accessing websites with the intent to access “chat-rooms”, “Facebook”, or unsupervised e-mail facilities.

Communicating E-Safety

Introducing the e-safety policy to students
Safety rules will be taught to all students in Year 7, and repeated each year as part of the ICT curriculum.

All system users will be informed that network and Internet use will be monitored. A programme of e-safety training and awareness raising will be put in place by September 2017.

Enlisting parents’ and carers support
Parents’ and carers’ attention will be drawn to the College e-safety Policy in Newsletters, the College prospectus and on the College. Parents can also pick up useful tips on e-safety on the Website. A parental guide is available for all parents on the use of social networking

E-safety Assemblies
E-safety assemblies are delivered to students where the guidelines for e-safety are reinforced and the College stance against any form of bullying is reinforced.
Education and Training

Uplands teaches students in line with the ‘Education for a Connected World’ Framework found here: [https://www.gov.uk/government/publications/education-for-a-connected-world](https://www.gov.uk/government/publications/education-for-a-connected-world)

In **Key Stage 3**, pupils will be taught to:

- Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy;
- Recognise inappropriate content, contact, and conduct, and know how to report concerns.

Pupils in **Key Stage 4** will be taught:

- To understand how changes in technology affect safety, including new ways to protect their online privacy and identity;
- How to report a range of concerns.

The safe use of social media and the internet will also be covered in other subjects where relevant.

The College will use assemblies to raise pupils’ awareness of the dangers that can be encountered online and may also invite speakers to talk to pupils about this.

**Parents**

The College will raise parents’ awareness of internet safety in letters or other communications home, and in information via our website or virtual learning environment (VLE).

This policy will also be shared with parents.

Online safety will also be covered during parents’ evenings.

If parents have any queries or concerns in relation to online safety, these should be raised in the first instance with the Principal and/or the DSL.

Concerns or queries about this policy can be raised with any member of staff or the Principal.

**E-safety education** will be provided in the following ways:

- A planned e-safety programme is provided as part of the advisor and assembly programme and is regularly revisited in Information Technology and other lessons across the curriculum – this programme covers both the use of ICT and new technologies in the College and outside of the College;
- Students are taught in lessons to be critically aware of the materials/content they access on-line and are guided to validate the accuracy of the information;
- Students are helped to understand the need for the Pupil AUP and encouraged to adopt safe and responsible use of ICT, the Internet and mobile devices both within and outside of College;
- Students are taught to acknowledge the source of information used and to respect copyright when using material accessed on the Internet;
- Rules for the use of ICT systems and the Internet are posted in College;
- Staff act as good role models in their use of ICT, the Internet and mobile devices.
Acceptable usage policy

- **Parents/carers** will be required to read through and sign alongside their child’s signature, helping to ensure their children understand the rules;
- **Staff and regular visitors** to the College have an AUP that they must read through and sign to indicate understanding of the rules.

Staff training

- E-safety coordinator ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- E-safety coordinator will be trained by CEOP as a CEOP ambassador to allow for the training of key staff to be Thinkuknow trainers and therefore educate pupils effectively;
- A planned programme of e-safety training is available to all **staff**. An audit of the e-safety training needs of all staff will be carried out regularly;
- All new **staff** receive e-safety training as part of their induction programme, ensuring that they fully understand the College E-Safety Policy, Acceptable Usage and Child Protection Policies;
- The **E-Safety Coordinator/SLT link** will receive regular updates through Local Authority and/or other information/training sessions and by reviewing guidance documents released;
- **Governors** are invited to take part in e-safety training and awareness sessions, with particular importance for those who are members of any committee or working group involved in ICT, e-safety, health and safety or child protection.

Social Networking Sites

Young people will not be allowed on social networking sites at the College; at home, it is the parental responsibility, but parents should be aware that it is illegal for children under the age of 13 to be on certain social networking sites.

- **Staff** should not access social networking sites on the College equipment in the College or at home. Staff should access sites using personal equipment;
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the College community on any social networking site or blog;
- **Students/parents/carers** should be aware the College will investigate misuse of social networking if it impacts on the well-being of other students or stakeholders;
- If inappropriate comments are placed on social networking sites about the College or College staff then advice would be sought from the relevant agencies, including the police if necessary;
- Students in the Key Stage 3 curriculum will be taught about e-safety on social networking sites as we accept some may use it outside of the College.

Monitoring

All use of the College’s Internet access is logged and the logs are randomly but regularly monitored by the ICT Department. Whenever any inappropriate use is detected it will be followed up by the E-Safety Co-ordinator, Student Managers, Progress Leaders, or members of the Senior Leadership Team depending on the severity of the incident.

- ICT Network Manager will maintain the Change Control Log and record any breaches, suspected or actual, of the filtering systems;
Any member of staff employed by the College who comes across an e-safety issue does not investigate any further but immediately reports it to the e-safety co-ordinator and impounds the equipment. This is part of the College safeguarding protocol. (If the concern involves the E-Safety Co-ordinator then the member of staff should report the issue to the Principal).

**Incident Reporting**

Any e-safety incidents must immediately be reported to the Principal (if a member of staff) or the E-Safety Coordinator (if a student) who will investigate further following e-safety and safeguarding policies and guidance.

**Responding to incidents of misuse**

It is hoped that all members of the College community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place through careless or irresponsible, or very rarely, through deliberate misuse. If any apparent or actual, misuse appears to involve illegal activity e.g. child sexual abuse images, adult material which potentially breaches the Obscene Publications Act, criminally racist material or other criminal conduct, activity or materials the flow chart should be consulted. Actions will be followed in accordance with policy, in particular the sections on reporting the incident to the police and the preservation of evidence. If members of staff suspect that misuse might have taken place, but that the misuse is not illegal (as above) it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation. It is recommended that more than one member of staff is involved in the investigation which should be carried out on a “clean” designated computer. It is more likely that the College will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the College community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures.

<table>
<thead>
<tr>
<th>Sanctions Type of site</th>
<th>Action Taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Games sites during lesson time</td>
<td>Student taken off the site. Class teacher/Curriculum Area Leader to apply sanctions</td>
</tr>
<tr>
<td>Social networking</td>
<td>All sites are banned.</td>
</tr>
<tr>
<td>Bullying via email messages</td>
<td>Internet use suspended. Sanctions applied by Curriculum Area Leader/Inclusion Team. Parents informed.</td>
</tr>
<tr>
<td>Pornography</td>
<td>As above. Report to IT Technicians to remove site. Inform IWF. Principal informed. Sanctions applied if applicable</td>
</tr>
<tr>
<td>Intolerance</td>
<td>Internet use suspended. Sanctions applied by Curriculum Area Leader/Inclusion Team. Parents informed.</td>
</tr>
<tr>
<td>Gambling</td>
<td>All sites are banned.</td>
</tr>
<tr>
<td>Proxy by pass</td>
<td>Internet use suspended. Class teacher/ Curriculum Area Leader to apply sanctions.</td>
</tr>
</tbody>
</table>
Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins and staff meetings).

The DSL and deputies will undertake child protection and safeguarding training, which will include online safety, at least every two years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Governors will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our child protection and safeguarding policy.
Appendix 1 - Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the College currently considers the benefit of using these technologies for education outweighs their risks/disadvantages:

<table>
<thead>
<tr>
<th>Communication Technologies</th>
<th>Staff and other adults</th>
<th>Students and young people</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Permitted</td>
<td>Permitted at certain times</td>
</tr>
<tr>
<td>Mobile phones May be brought to the College</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Mobile phones used in lessons</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Use of mobile phones in social time (break time and lunchtime)</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Taking photographs on mobile devices</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Use of PDAs and other educational mobile devices</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use of the College email for personal emails</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Social use of chat rooms/facilities</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Use of social network sites</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Use of educational blogs</td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>

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

- The official College email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the College email service to communicate with others when in the College, or on the College systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to the nominated person (in accordance with the College policy) the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email;
- Any digital communication between staff and pupils or parents/carers (email, chat, Learning Platform etc.) must be professional in tone and content. These communications may only take place on official (monitored) College systems. Personal email addresses,
text messaging or public chat/social networking programmes must not be used for these communications;

- Students should be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Personal information should not be posted on the College website and only official email addresses should be used to identify members of staff.

**Appendix 2 - Unsuitable / inappropriate activities**

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from the College and all other ICT systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities, which may, generally, be legal but would be inappropriate in a College context, either because of the age of the users or the nature of those activities. The College believes that the activities referred to in the following section would be inappropriate in a College context and that users, as defined below, should not engage in these activities in the College or outside the College when using College equipment or systems. The College policy restricts certain internet usage as follows. Users shall not visit internet sites, make, post, download, upload, data transfer, communicate, or pass on, material, remarks, proposals, or comments that contain or relate to:

<table>
<thead>
<tr>
<th>User actions</th>
<th>Acceptable</th>
<th>Acceptable at certain times</th>
<th>Acceptable for nominated users</th>
<th>Unacceptable</th>
<th>Unacceptable and illegal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Child sexual abuse images</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Adult material that potentially breaches the Obscene Publications Act in the UK</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Criminally racist material in the UK</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Pornography</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Promotion of any kind of discrimination</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Promotion of racial or religious hatred</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Threatening behaviour, including promotion of physical violence or mental harm</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the College or brings the College into disrepute</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Using College systems to run a private business</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Uplands College</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Creating or propagating computer viruses or other harmful files</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files) that causes network congestion and hinders others in their use of the internet</td>
<td></td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Incident involving students</td>
<td>Teacher to use College behaviour policy to deal with</td>
<td>Refer to Student HoD/ E-Safety Coordinator</td>
<td>Refer to police</td>
<td>Refer to technical support staff for action re security/filtering etc.</td>
<td></td>
</tr>
<tr>
<td>-----------------------------</td>
<td>---------------------------------------------------</td>
<td>------------------------------------------</td>
<td>----------------</td>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities).</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of non-educational sites during lessons</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of mobile phone/ digital camera/ other handheld device.</td>
<td>X</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unauthorised use of social networking/ instant messaging/ personal email</td>
<td>X</td>
<td>X</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Unauthorised downloading or uploading of files</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Allowing others to access College network by sharing username and passwords</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Attempting to access or accessing the College network, using another student's account</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Attempting to access or accessing the College network, using the account of a member of staff</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Corrupting or destroying the data of other users</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Continued infringements of the above, following previous warnings or sanctions</td>
<td>X</td>
<td>Community Police Officer referral</td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Actions which could bring the College into disrepute or breach the integrity of the ethos of the College</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Using proxy sites or other means to subvert the College's filtering system</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Accidentally accessing offensive or pornographic material and failing to report the incident</td>
<td>X</td>
<td></td>
<td></td>
<td>X</td>
<td></td>
</tr>
</tbody>
</table>
Appendix 3

The guidance in this policy should be implemented with cross reference to the College’s Child Protection, Anti-Bullying and Behaviour Policies.

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.

<table>
<thead>
<tr>
<th>Student:</th>
<th>Form:</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Signed:</th>
<th>Date:</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Signed:</th>
<th>Date:</th>
</tr>
</thead>
</table>

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.

<table>
<thead>
<tr>
<th>Signed:</th>
<th>Date:</th>
</tr>
</thead>
</table>

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 Principal;
- 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: ........
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 encyclopedias 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 College’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 College 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 College, external contractors providing services on behalf of the College or the County Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the College. 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 College purposes; including sites hosted and maintained on behalf of the College (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, microblogs 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 College 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:
  o The Human Rights Act 1998;
  o Common law duty of confidentiality, and
  o The Data Protection Act 1998.
● Confidential information includes, but is not limited to:
  o Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998;
  o Information divulged in the expectation of confidentiality;
  o College or County Council business or corporate records containing organisationally or publicly sensitive information;
  o Any commercially sensitive information such as information relating to commercial proposals or current negotiations, and
  o 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

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 College 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 College 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 College or County Council in their personal webspace. This is to prevent information on these sites from being linked with the College 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 College 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 College and through official College 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 College 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 Colleges 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 the College 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 the College or County Council uniforms or clothing with the College or County Council logos or images identifying sensitive College or County Council premises (e.g. care homes, secure units) must not be published on personal webspace;

● The College 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 encyclopedias 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 College 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 College sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the College to unwelcome publicity or cause reputational damage;
• Official College 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 College’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 College 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 College 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, College staff or members of the public will be able to contribute content to the site, must be discussed with the College’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 Principal 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 College’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 College 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 College. 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 Principal;
- 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 Principal;
- 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 Principal;
- The Deputy Head of ICT Strategy must be consulted about the purpose of the proposed site and its content. In addition, the Principal’s approval must be obtained for the use of the College 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 Principal immediately. Staff members must not communicate with the media without the advice or approval of the Principal.

**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 College 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 College’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 College logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the College 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 College 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 College’s Principal;
- Approval must also be obtained from the College’s Deputy Principal 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 College’s Deputy Principal of ICT Strategy.

<table>
<thead>
<tr>
<th>TEAM DETAILS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Department</td>
</tr>
<tr>
<td>Name of author of site</td>
</tr>
<tr>
<td>Author’s line manager</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PURPOSE OF SETTING UP SOCIAL MEDIA SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>(please describe why you want to set up this site and the content of the site)</td>
</tr>
<tr>
<td>What are the aims you propose to achieve by setting up this site?</td>
</tr>
<tr>
<td>What is the proposed content of the site?</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROPOSED AUDIENCE OF THE SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please tick all that apply.</td>
</tr>
<tr>
<td>☐ Pupils of Uplands Community College</td>
</tr>
<tr>
<td>☐ Uplands Community College staff</td>
</tr>
<tr>
<td>☐ Pupils’ family members</td>
</tr>
<tr>
<td>☐ Pupils from other schools (provide names of schools)</td>
</tr>
<tr>
<td>☐ External organisations</td>
</tr>
<tr>
<td>☐ Members of the public</td>
</tr>
<tr>
<td>☐ Others; please provide details</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>PROPOSED CONTRIBUTORS TO THE SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Please tick all that apply.</td>
</tr>
<tr>
<td>☐ Pupils of Uplands Community College</td>
</tr>
<tr>
<td>☐ Uplands Community College staff</td>
</tr>
<tr>
<td>☐ Pupils’ family members</td>
</tr>
<tr>
<td>☐ Pupils from other schools (provide names of schools)</td>
</tr>
<tr>
<td>☐ External organisations</td>
</tr>
<tr>
<td>☐ Members of the public</td>
</tr>
<tr>
<td>☐ Others; please provide details</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ADMINISTRATION OF THE SITE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Names of administrators</td>
</tr>
</tbody>
</table>
(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 Principal).

<table>
<thead>
<tr>
<th><strong>Line Manager</strong></th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>I approve the aims and content of the proposed site.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Deputy Head ICT Strategy</strong></th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>I approve the aims and content of the proposed site.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Principal</strong></th>
<th>Name</th>
<th>Signature</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>I approve the aims and content of the proposed site and the use of College brand and logo.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
**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.

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