UPLANDS COMMUNITY COLLEGE

E-Safety Policy (including social media)

Document title	E-Safety Policy
Policy number	S024
Version number	1.1
Policy status	Approved
Date of issue	August 2018
Date to be revised	August 2019
Owner	Carly Sargeant
Author	Liam Collins and Carly Sargeant

Revision log (last 5 changes)

Date	**Version No**	**Brief detail of change**
28/08/18	1.1	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

Contents

1 Creating an online safety ethos

1.1 Aims

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital 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.

Uplands Community College:

- Believes that online safety (e-Safety) is an essential element of safeguarding children and adults in the digital world, when using technology such as computers, tablets, mobile phones or games consoles;
- Identifies that the internet and information communication technologies are an important part of everyday life, so children must be supported to be able to learn how to develop strategies to manage and respond to risk and be empowered to build resilience online;
- Has a duty to provide the school community with quality Internet access to raise education standards, promote pupil achievement, support professional work of staff and enhance the schools management functions;
- Identifies that there is a clear duty to ensure that children are protected from potential harm online.

Uplands Community 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 school community in its use of technology;
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate.

This policy applies to:

- All staff including the governing board, teachers, support staff, external contractors , visitors, volunteers and other individuals who work for or provide services on behalf of the school (collectively referred to as 'staff' in this policy) as well as children and parents/carers;
- All access to the internet and use of information communication devices including personal devices or where children, staff or other individuals have been provided with school issued devices for use off-site, such as a work laptops, tablets or mobile phones.

This policy must be read in conjunction with other relevant school policies including (but not limited to) Safeguarding and Child Protection, Anti-Bullying, Behaviour, Data Security, Image Use, Acceptable Use Policies, Confidentiality, Screening, Searching and Confiscation and relevant curriculum policies including cComputing, Personal Social and Health Education (PSHE), Citizenship and Sex and Relationships Education (SRE).

1.2 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.

1.3 Writing and reviewing

The Designated Safeguarding Lead (DSL) is Carly Sargeant, as of 31st October, 2018. However, Caroline Kelly (Behaviour and Safeguarding Manager) currently has this responsibility with full knowledge of SLES.

The school online safety (e-safety) lead for the Governing Board is Jason Scott-Taggart.

- Uplands' online safety policy has been written by the school, involving staff, pupils and parents/carers, building on the East Sussex County Council (ESCC) online safety policy template, with specialist advice and input as required;
- The policy has been approved and agreed by the Leadership Team and Governing Body.
- The school has appointed the Designated Safeguarding Lead as an appropriate member of the leadership team and the online safety lead;
- The school has appointed a member of the Governing Body to take lead responsibility for online safety (e-Safety);
- The online safety (e–Safety) Policy and its implementation will be reviewed by the school at least annually or sooner if required.

1.4 Key responsibilities of the community

1.4.1 Senior Leadership Team, including Headteacher

- Developing, owning and promoting the online safety vision and culture to all stakeholders, in line with national and local recommendations with appropriate support and consultation throughout the school community;
- Ensuring that online safety is viewed by the whole community as a safeguarding issue and proactively developing a robust online safety culture.
- Supporting the DSL by ensuring they have sufficient time and resources to fulfil their online safety role and responsibilities;
- Auditing and evaluating current online safety practice to identify strengths and areas for improvement;

- Ensuring there are appropriate and up-to-date policies and procedures regarding online safety including an Acceptable Use Policy, which covers appropriate professional conduct and use of technology.;
- To ensure that suitable and appropriate filtering and monitoring systems are in place to protect children from inappropriate content which meet the needs of the school community whilst ensuring children have access to required educational material;
- To work with and support technical staff in monitoring the safety and security of school systems and networks and to ensure that the school network system is actively monitored;
- Ensuring all members of staff receive regular, up-to-date and appropriate training regarding online safety roles and responsibilities and provide guidance regarding safe appropriate communications;
- Ensuring that online safety is embedded within a progressive whole school curriculum which enables all pupils to develop an age-appropriate understanding of online safety and the associated risks and safe behaviours;
- Making appropriate resources available to support the development of an online safety culture;
- Taking responsibility for online safety incidents and liaising with external agencies and support as appropriate;
- Receiving and regularly reviewing online safety incident logs and using them to inform and shape future practice;
- Ensuring there are robust reporting channels for the school/setting community to access regarding online safety concerns, including internal, local and national support;
- Ensure that appropriate risk assessments are undertaken regarding the safe use of technology, including ensuring the safe and responsible use of devices;
- To ensure a member of the Governing Board is identified with a lead responsibility for supporting online safety;
- To ensure that the DSL works in partnership with the e-safety lead and Network Manager.

1.4.2 Designated Safeguarding Lead

Details of the school’s Designated Safeguarding Lead (DSL) and deputies are set out in our Child Protection and Safeguarding Policy.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school;
- Working with the Headteacher, ICT Network Manager and other staff, as necessary, to address any online safety issues or incidents;
- Ensuring that any online safety incidents are logged 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 school behaviour policy;
- Updating and delivering staff training on online safety;
- Liaising with other agencies and/or external services if necessary;
- Providing regular reports on online safety in school to the Headteacher and/or governing board;
- Acting as a named point of contact on all online safeguarding issues and liaising with other members of staff and other agencies as appropriate;
- Keeping up-to-date with current research, legislation and trends regarding online safety;

- Coordinating participation in local and national events to promote positive online behaviour, e.g. Safer Internet Day;
- Ensuring that online safety is promoted to parents and carers and the wider community through a variety of channels and approaches;
- Work with the school lead for data protection and data security to ensure that practice is in line with current legislation;
- Maintaining a record of online safety concerns/incidents and actions taken as part of the school's safeguarding recording structures and mechanisms;
- Monitor online safety incidents to identify gaps/trends and use this data to update the school/settings education response to reflect need;
- Liaising with the local authority and other local and national bodies, as appropriate;
- Reviewing and updating online safety policies, Acceptable Use Policies (AUPs) and other related procedures on a regular basis (at least annually) with stakeholder input;
- Ensuring that online safety is integrated with other appropriate school policies and procedures;
- Leading an online safety team/group with input from all stakeholder groups;
- Meet regularly with the governor/board/committee member with a lead responsibility for online safety.

This list is not intended to be exhaustive.

1.4.3 The ICT Network Manager

The ICT Network Manager is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep pupils safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material;
- Ensuring that the school'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 school'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 and dealt with appropriately in line with this policy;
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy;
- Report any breaches or concerns to the DSL and leadership team and together ensure that they are recorded and appropriate action is taken as advised.
- Developing an understanding of the relevant legislation as it relates to the security and safety of the technical infrastructure;
- Report any breaches and liaising with the local authority (or other local or national bodies) as appropriate on technical infrastructure issues;
- Providing technical support and perspective to the DSL and leadership team, especially in the development and implementation of appropriate online safety policies and procedures;
- Ensuring that appropriate anti-virus software and system updates are installed and maintained on all setting machines and portable devices;

- Ensure that appropriately strong passwords are applied and enforced for all.

This list is not intended to be exhaustive.

1.4.4 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 school's ICT systems and the internet, and ensuring that pupils follow the school's terms on acceptable use;
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy;
- Having an awareness of a range of online safety issues and how they relate to the children in their care;
- Modelling good practice when using new and emerging technologies;
- Embedding online safety education in curriculum delivery wherever possible;
- Identifying individuals of concern and taking appropriate action by following school safeguarding policies and procedures;
- Knowing when and how to escalate online safety issues, internally and externally;
- Being able to signpost to appropriate support available for online safety issues, internally and externally;
- Maintaining a professional level of conduct in their personal use of technology, both on and off site;
- Demonstrating an emphasis on positive learning opportunities.

This list is not intended to be exhaustive.

1.4.5 Students

- Contributing to the development of online safety policies;
- Reading the school/setting Acceptable Use Policies (AUPs) and adhering to them;
- Respecting the feelings and rights of others both on and offline;
- Seeking help from a trusted adult if things go wrong, and supporting others that may be experiencing online safety issues;
- Taking responsibility for keeping themselves and others safe online;
- Taking responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies;
- Assessing the personal risks of using any particular technology, and behaving safely and responsibly to limit those risks.

1.4.6 Parents and carers

Parents/carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this policy;
- Ensure their child has read, understood, and agreed to the terms on acceptable use of the school'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
Hot topics, Childnet International: http://www.childnet.com/parents-and-carers/hot-topics
Parent factsheet, Childnet International: http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf

1.4.7 Visitors and members of the community

Visitors and members of the community who use the school'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.

2 Online Communication and Safer Use of Technology

2.1 Managing the school website

- The school will ensure that information posted on the school website meets the requirements as identified by the Department for Education;
- The contact details on the website will be the school address, email and telephone number. Staff or pupils' personal information will not be published;
- The head teacher will take overall editorial responsibility for online content published by the school and will ensure that content published is accurate and appropriate;
- The school website will comply with the school's guidelines for publications including respect for intellectual property rights, privacy policies and copyright;
- Pupils work will be published with their permission or that of their parents/carers;
- The administrator account for the school website will be safeguarded with an appropriately strong password;
- The school will post information about safeguarding, including online safety, on the school website for members of the community.

2.2 Publishing videos and images online

- The school will ensure that all images and videos shared online are used in accordance with the school image use policy;
- The school/setting will ensure that all use of images and videos take place in accordance other policies and procedures including data security, Acceptable Use Policies, Codes of Conduct, social media, use of personal devices and mobile phones etc.;
- In line with the image policy, written permission from parents or carers will always be obtained before images/videos of pupils are electronically published.

2.3 Email

- Pupils may only use school/setting provided email accounts for educational purposes;

- All members of staff are provided with a specific school/setting email address to use for any official communication;
- The use of personal email addresses by staff for any official school/setting business is not permitted;
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider;
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using secure and encrypted email, e.g. communication with ESBAS and other children's services;
- Members of the community must immediately tell a designated member of staff if they receive offensive communication and this will be recorded in the school safeguarding files/records;
- Email sent to external organisations should be written carefully and authorised before sending, in the same way as a letter written on school headed paper would be;
- The school will have a dedicated email for reporting wellbeing and pastoral issues. This inbox will be managed by designated and trained staff;
- School email addresses and other official contact details will not be used for setting up personal social media accounts.

2.4 Appropriate and safe classroom use of the internet

- Internet use is a key feature of educational access and all children will receive age and ability appropriate education to support and enable them to develop strategies to respond to concerns as part of an embedded whole school curriculum. Please access curriculum policies for further information.
- The school's internet access will be designed to enhance and extend education.
- Access levels to the internet will be reviewed to reflect the curriculum requirements and the age and ability of pupils.
- All members of staff are aware that they cannot rely on filtering alone to safeguard children and supervision, classroom management and education about safe and responsible use is essential.
- Supervision of pupils will be appropriate to their age and ability.
- All school owned devices will be used in accordance with the school Acceptable Use Policy and with appropriate safety and security measure in place.
- Members of staff will always evaluate websites, tools and apps fully before use in the classroom or recommending for use at home.
- Pupils will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.
- The school will use age appropriate search tools.
- The school will ensure that the use of Internet-derived materials by staff and pupils complies with copyright law and acknowledge the source of information.
- Pupils will be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy;
- The evaluation of online materials is a part of teaching and learning in every subject and will be viewed as a whole-school/setting requirement across the curriculum;

- The school will use the internet to enable pupils and staff to communicate and collaborate in a safe and secure environment.

3 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 school 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 school 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 school 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.

3.1 E-safety and anti-bullying

The e-safety policy has links with the schools 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;
- Feedback from survey and questionnaires issued to students, parents and carers and staff.

4 Cyber-bullying

4.1 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 school Behaviour Policy.)

4.2 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 school 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.

The school 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 school will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among pupils, the school 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.

4.3 Examining electronic devices

School 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 school 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 school 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 school complaints procedure.

5 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 email facilities.

6 Communicating E-Safety

6.1 Introducing the E-Safety Policy to students

Safety rules will be taught to all students in Year 7, and repeated in 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 2018.

6.2 Enlisting parents' and carers support

Parents' and carers' attention will be drawn to the school E-Safety Policy in newsletters, the school prospectus and on the school. 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.

6.3 E-safety Assemblies

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

7 Education and Training

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 school 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.

7.1 Parents

The school will raise parents' awareness of internet safety in letters or other communications home, and in information via our website or report portal.

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 Headteacher and/or the DSL.

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

7.2 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 school and outside of school;
- 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 school;
- 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 school;
- Staff act as good role models in their use of ICT, the Internet and mobile devices.

8. 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 school have an AUP that they must read through and sign to indicate understanding of the rules;
- All use of mobile phones and personal devices by children will take place in accordance with the acceptable use policy;
- Pupil's personal mobile phones and personal devices will be kept in a student's bag, switched off and kept out of sight during lessons and while moving between lessons.
- Mobile phones or personal devices will not be used by pupils during lessons or formal school time unless as part of an approved and directed curriculum based activity with consent from a member of staff. The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted;
- If members of staff have an educational reason to allow children to use their mobile phones or personal devices as part of an educational activity then it will only take place when approved by the Senior Leadership Team;
- If a pupil needs to contact his/her parents/carers they will be allowed to use a school phone;
- Parents are advised not to contact their child via their mobile phone during the school day, but to contact the school office. Exceptions may be permitted in exceptional circumstances on a case-by-case basis and as approved by the Headteacher;
- Pupils should protect their phone numbers by only giving them to trusted friends and family members;
- Pupils will be instructed in safe and appropriate use of mobile phones and personal devices and will be made aware of boundaries and consequences;
- Mobile phones and personal devices must not be taken into examinations. Pupils found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the pupil's withdrawal from either that examination or all examinations;
- If a pupil breaches the school policy then the phone or device will be confiscated and will be held in a secure place in SST Office. Mobile phones and devices will be released to parents/carers in accordance with the school policy;
- School staff may confiscate a pupil's mobile phone or device if they believe it is being used to contravene the schools behaviour or bullying policy. The phone or device may be searched by a member of the Leadership team with the consent of the pupil or parent/carer. Searches of mobile phone or personal devices will be carried out in accordance with the schools policy. If there is suspicion that material on a pupil's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence then the device will be handed over to the police for further investigation.

9. Staff 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.

- The E-Safety Co-ordinator will ensure that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- The Network Manager and DSL 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 relating to safeguarding, ensuring that they fully understand the school E-Safety Policy, Acceptable Usage and Child Protection Policies;
- The **E-Safety Co-ordinator/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.

The following links are useful for staff:

- (childnet.com) Teachers and Professionals - for you as a professional
- (childnet.com) Teachers and Professionals Professional Reputation
- (saferinternet.org.uk) Teachers and Professionals Professional Reputation

10 Social Networking Sites

Young people will not be allowed on social networking sites at school as mobile phones are not permitted; 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 school equipment in school or at home. Staff should access sites using personal equipment, outside of school;
- **Staff** users should not reveal names of staff, students, parents/carers or any other member of the school community on any social networking site or blog**;**
- **Students/parents/carers** should be aware the school 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 school or school staff then advice would be sought from the relevant agencies, including the police if necessary;
- Students will be taught about e-safety on social networking sites as we accept some may use it outside of school.

10.1 Monitoring

All use of the school'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 school 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 school safeguarding protocol. (If the concern involves the E-Safety Co-ordinator then the member of staff should report the issue to the Headteacher).

10.2 Incident Reporting

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

10.3 Responding to incidents of misuse

It is hoped that all members of the school 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 school 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 school 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.

Sanctions type of site	**Action taken**
Games sites during lesson time	Student taken off the site. Class teacher/Curriculum Area Leader to apply sanctions
Social networking	All sites are banned.
Bullying via email messages	Internet use suspended. Sanctions applied by Curriculum Area Leader/Inclusion Team. Parents informed.
Pornography	As above. Report to IT Technicians to remove site. Inform IWF. Headteacher informed. Sanctions applied if applicable and parents informed.

Intolerance	Internet use suspended. Sanctions applied by Curriculum Area Leader/Inclusion Team. Parents informed.
Gambling	All sites are banned
Proxy by-pass	Internet use suspended. Class teacher/ Curriculum Area Leader to apply sanctions.

Appendix 1 - Communications

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

		Staff and other adults					Students and young people			
Communication Technologies		Permitted	Permitted at certain times	Permitted for named staff	Not Permitted		Permitted	Permitted at certain times	Allowed with staff permission	Not Permitted
Mobile phones May be brought to school		X					X			
Mobile phones used in lessons					X				X	
Use of mobile phones in social time (break time and lunchtime)		X								X
Taking photographs on mobile devices					X					X
Use of PDAs and other educational mobile devices		X							X	
Use of school email for personal emails					X					X
Social use of chat rooms/facilities					X					X
Use of social network sites				X						X
Use of educational blogs		X					X			

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

- The official school email service may be regarded as safe and secure and is monitored. Staff and students should therefore use only the school email service to communicate with others when in school, or on school 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 school 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) school 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 school 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 school 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 school context, either because of the age of the users or the nature of those activities. The school believes that the activities referred to in the following section would be inappropriate in a school context and that users, as defined below, should not engage in these activities in school or outside school when using school equipment or systems. The school 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:

User actions	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Child sexual abuse images					X
Promotion or conduct of illegal acts, e.g. under the child protection, obscenity, computer misuse and fraud legislation					X
Adult material that potentially breaches the Obscene Publications Act in the UK					X
Criminally racist material in the UK					X
Pornography					X
Promotion of any kind of discrimination				X	
Promotion of racial or religious hatred					X
Threatening behaviour, including promotion of physical violence or mental harm					X
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the school or brings the school into disrepute				X	
Using school systems to run a private business				X	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by Uplands school				X	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				X	
Revealing or publicising confidential or proprietary information (eg financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
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				X	
On-line gaming (educational)		X			
On-line gaming (non- educational)				X	
On-line gambling				X	
On-line shopping / commerce			X		
File sharing			X		
Use of social networking sites			X		
Downloading video broadcasting e.g. YouTube	X				

<u>Incident involving students</u>	**Teacher to use school behaviour policy to deal with**	**Refer to student HoD/ E-Safety Coordinator**	**Refer to police**	**Refer to technical support staff for action re security/filtering etc.**
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities**).**		X	X	X
Unauthorised use of non-educational sites during lessons	X			X
Unauthorised use of mobile phone/ digital camera/ other handheld device.	X			
Unauthorised use of social networking/ instant messaging/ personal email	X	X		X
Unauthorised downloading or uploading of files		X		X
Allowing others to access school network by sharing username and passwords		X		X
Attempting to access or accessing the school network, using another student's account		X		X
Attempting to access or accessing the school network, using the account of a member of staff		X		X
Corrupting or destroying the data of other users		X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature		X		X
Continued infringements of the above, following previous warnings or sanctions		X	Community Police Officer referral	X
Actions which could bring the school into disrepute or breach the integrity of the ethos of the school		X		X
Using proxy sites or other means to subvert the school's filtering system		X		X
Accidentally accessing offensive or pornographic material and failing to report the incident		X		X
Uploading to video broadcast e.g. YouTube			X	

Appendix 3: E-safety Rules and Staff Code of Conduct

The guidance in this policy should be implemented with cross reference to the School'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.

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 Co-ordinator or the Designated Child Protection Co-ordinator;
- 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: ………

11. Social Media Policy

11.1 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 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.

11.2 Scope

- This policy applies to Uplands Community College governing board, 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;
- 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.

11.3 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 cyber-bullying 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.

11.4 Related policies

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

11.5 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.

11.6 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 Appendix 1;
- 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 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;
- The use of social networking applications during school hours for personal use **is not** permitted without explicit permission. Use of social media during school/work hours or whilst using school devices may result in disciplinary or legal action and/or removal of Internet facilities;
- Any concerns regarding the online conduct of any member of Uplands community on social media sites should be reported to the leadership team and will be managed in accordance with policies such as anti-bullying, allegations against staff, behaviour and safeguarding/child protection;
- Any breaches of school/setting policy may result in criminal, disciplinary or civil action being taken and this will depend upon the age of those involved and the circumstances of the wrong committed. Action taken will be accordance with relevant policies, such as anti-bullying, behaviour, safeguarding and child protection including the allegations against staff section.

11.7 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 1 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.

11.8 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.

11.9 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 Senior Leadership Team;
- 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 the Senior Leadership Team.

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 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, and the Senior Leadership Team;
- Content contributed to own or third-party hosted sites must be discussed with and approved by the staff member's line manager, and the Senior Leadership Team;
- The Senior Leadership Team 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 2) and forward it to the Senior Leadership Team 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 Senior Leadership Team 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 Senior Leadership Team.

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

ADMINISTRATION 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	
Senior Leadership Team **I approve the aims and content of the proposed site.**	Name	
	Signature	
	Date	
Headteacher	Name	
	Signature	

I approve the aims and content of the proposed site and the use of school brand and logo.	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 Co-ordinator 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 Senior 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