7a.2 Online Policy & Social Media Policy

Author:	Andrew Wilkes
Last review:	August 2020
Next review:	September 2021
Approved by:	C M Reynolds
Document:	v4

Online Policy

1 Background and Rationale

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. At home, technology is changing the way children live and activities in which they choose to partake. These trends are set to continue.

While developing technology brings many opportunities, it also brings risks and potential dangers of which these are just a few:

- Access to illegal, harmful or inappropriate images or other content
- Allowing or seeking unauthorised access to personal information
- Allowing or seeking unauthorised access to private data, including financial data
- The risk of being subject to grooming by those with whom they make contact on the internet
- The risk of coming into contact with extremist material posted with the aim of radicalising individuals
- The sharing / distribution of personal images without an individual's consent or knowledge
- Inappropriate communication / contact with others, including strangers
- Cyber-bullying/ sexting and banter / peer on peer abuse
- 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 or addictive use which may impact on social and emotional development and learning.

This policy sets out how we strive to keep children safe with technology while they are at University College School. We recognise that children may be more at risk when using technology at home (where we have no control over the technical structures put in place to keep them safe) and so this policy also sets out how we educate children about the potential risks.

Our Online Policy has been derived from a model provided by the South West Grid for Learning.

2 Responsibilities

Responsibility for online safety at the school lies with the Deputy Head Pastoral, who is the Designated Safeguarding Lead.

The school's Senior Management Team is responsible for the provision of ICT at UCS.

The Technical Services Manager, is responsible for the development and maintenance of the ICT network, and reports to the Director of Operations. The IT support staff are responsible for ensuring that

- UCS's ICT infrastructure and data are secure and not open to misuse or malicious attack
- Users may only access the network through the use of a password
- Shortcomings in the infrastructure are reported to the Technical Services Manager so that appropriate action might be taken

The Technical Services Manager is also responsible for the management, security and operation of the school's Management Information System; the SIMS Manager is responsible for the data held on this system and reports to the Vice Master.

The Head Librarian is responsible for the use of ICT in the Library, and reports to the Deputy Head (Academic).

The Head of the Academic ICT Department reports to the Deputy Head (Academic).

Classroom-based staff – teaching and support staff – are responsible for ensuring that

- They safeguard the welfare of children and refer child protection concerns using the proper channels
- They promote online safety in connection with any curricular work which may involve the use of ICT
- They have an up-to-date awareness of online-safety matters and of the school's current Online Policy and practices
- They report any suspected misuse or problem to a member of the IT support staff
- They undertake that any digital communications with pupils (email / Firefly, Twitter, etc) should be conducted in a fully professional manner and only using official school systems

Pupils are provided with access to the ICT network on arrival at the school. Breaches of protocol by pupils may be dealt with by their Form Teachers or Wardens; serious breaches of protocol by pupils may be dealt with by the Deputy Head Pastoral or by the Headmaster.

3 Scope of the Policy

This policy applies to all members of the school community (including teaching staff, support staff, pupils, volunteers, parents/carers, visitors and other users) who have access to and are users of the school's ICT systems, both in and out of school. Unless otherwise indicated, 'Pupils' refers to any current or prospective pupils and former pupils; 'Parents/carers' refers to current and prospective parents / carers.

The policy covers the use of all social media applications (e.g. Twitter, LinkedIn, YouTube, and Facebook), digital media sharing, personal emails, microblogs and blogs. It should also be noted that as the school uses Google Apps for Education, users are bound to the terms and conditions outlined by Google, which appear for every user on first logon.

Employees

The basic premise concerning social media sites is that all Employees need to exercise common sense and to realise that what is written on social media sites is essentially in the public domain i.e. even if privacy settings are in place or material is posted on a closed profile or group the information is essentially in the public domain. (As background information, ACAS's social media policy is centred on the principle of 'don't do anything on-line that you wouldn't do off-line' – the premise being not to stop Employees from conducting legitimate activities on the internet, but to flag up areas in which conflicts can arise, particularly those that impact on the organisation's reputation.)

Pupils

The Education and Inspections Act 2006 empowers Head Teachers, to such an extent as is reasonable, to regulate the behaviour of Pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online-safety incidents which may take place away from the school, but which are linked to membership of the school.

The school will deal with such incidents using guidance within this policy as well as associated Behaviour, Anti-bullying and Safeguarding Policies, and the UCS Code of Conduct, and will, where known, inform parents / carers of incidents of inappropriate online behaviour that take place away from UCS.

4 ICT and the UCS Code of Conduct

In the use of ICT, the UCS Code of Conduct towards other people must be respected.

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

Users must be polite and responsible when they communicate with others; it is not appropriate to employ aggressive or inappropriate language, and all users must respect the opinions and ideas of others.

Images or sound recordings of any member of the school community must not be taken or distributed without their permission.

5 Acceptable Use Agreement

An Acceptable Use Agreement is signed by pupils when they join the school. This will be repeated at the start of every year and a paper copy will be retained by the pupil's Form Tutor.

Employees are expected to abide by the terms of their employment contract and the policies and procedures contained within the Employment Reference File.

6 Personal Safety of Users

In the interests of all users' personal safety:

- The filtering of internet content provides an important means of preventing users from accessing material that is illegal or inappropriate in an educational context. The Technical Services Manager is responsible for the filtering of content.
- The school will monitor all use of the ICT systems and other digital resources. Staff may review files and communications to ensure that users are using the system responsibly. Users should not expect that files stored on servers or storage media are always private.
- Users may only access the system with their own secret login name and password. They must not attempt to log in to anyone else's account or seek to access their files. Members of staff should not ask pupils for their passwords.

- Pupils' personal information such as home address, telephone number, and name of their school should not be communicated via the school ICT system without the school's permission.
- Pupils need to be aware of the dangers of communicating digital images of themselves or others or posting such images on internet sites. Members of Staff are allowed to take digital still and video images to support educational aims but must not share, distribute or publish such images other than within the guidelines laid down by the school. Photographs of pupils may only be published by the school with their parents' permission, and never accompanied by the name of the pupil.
- If Pupils arrange to meet people off-line that they have communicated with on-line, they are strongly advised to do so in a public place and should take an accompanying adult.
- Employees who wish to use Twitter or other microblogging sites for school business must first obtain permission from the Assistant Head (Communications and Engagement) before creating a School Twitter account. All communications from this account must be in accordance with this policy and must not contain personal information.
- Users must not visit sites, make, post, download, upload, data transfer, communicate or pass on any material, remarks, proposals or comments that contain or relate to items that are illegal, defamatory, pornographic or otherwise offensive. Examples of offensive material include, but are not limited to:
    - **Child sexual abuse images** (illegal – The Protection of Children Act 1978)
    - **Grooming, incitement, arrangement or facilitation of sexual acts against children** (illegal – Sexual Offences Act 2003)
    - **Possession of extreme pornographic images** (illegal – Criminal Justice and Immigration Act 2008)
    - **Criminally racist material in the UK – to stir up religious hatred (or hatred on the grounds of sexual orientation)** (illegal – Public Order Act 1986)
    - **Sexting/youth produced sexual imagery**
    - **Upskirting**
    - Pornography
    - Promotion of any kind of discrimination
    - Promotion of racial or religious hatred
    - Promotion of terrorism
    - Threatening behaviour, including promotion of physical violence or mental harm
    - Any other information which may be offensive to other members of the UCS community, or which breaches the integrity of the school's ethos.

Pupils should report to an adult member of staff (Subject Teacher / Form Teacher/Tutor / Librarian / Technician) any material, information or messages that make them feel uncomfortable.

7 Risk from contact with violent extremists

Many extremist groups who advocate violence use the internet as a means of either inciting violence against specific groups or providing information on preparing explosives or carrying out terrorist acts. Because of their personal circumstances, some young people may be susceptible to these influences.

- Staff need to be aware of those pupils who are being targeted by or exposed to harmful influences from violent extremists via the internet. Pupils and staff should be warned of the risks of becoming involved in such groups and informed that accessing such websites is against school policies.

- In line with KCSIE [September 2020] the school will ensure that adequate filtering and monitoring is in place and will review filtering in response to any incident where a pupil or staff member accesses websites advocating violent extremism.
- All incidents should be dealt with as a breach of the acceptable use policies and the school's behaviour and staff disciplinary procedures should be used as appropriate.
- The Designated Safeguarding Lead should record and review all incidents in order to establish whether there are any patterns of extremist groups targeting the school and whether current school procedures are robust enough to deal with the issue.
- If there is evidence that the pupil is becoming deeply enmeshed in the extremist narrative, the school will act in accordance with the terms of the Safeguarding Policy and make a referral under the terms of the Prevent duty. See the UCS Safeguarding Policy.

Employees should report any misuse of the school's ICT systems to their Line Manager, the Technical services Manager, the Deputy Head (Pastoral) or the Headmaster.

If an Employee has access to the internet at the school, this should be used for educational purposes only. It will be considered to be an act of gross misconduct if they abuse the use of the internet by using it excessively for personal matters, or at all for accessing any offensive, obscene, pornographic, sexually explicit, or material that is discriminatory on the basis of age, race, religion or belief, sexual orientation, disability, gender reassignment or sex (this list is not exhaustive). Any such action will be treated very seriously and is likely to result in summary dismissal.
As anything written on any social media sites is regarded as being in the public domain, transmission of any material that in any way relates to the UCS Foundation and is considered as any of the following will constitute gross misconduct:

- Bringing the name of the UCS Foundation into disrepute or considered embarrassing to the Foundation;
- Defamatory;
- Offensive or obscene;
- Untrue or malicious;
- In breach of confidentiality or copyright.

8 Communication between Employees and Pupils / Employees and Parents

Employees' personal mobile/home telephone numbers should not normally be given to pupils or parents. This may only take place once written permission has been obtained from a member of SMT.

Texting pupils or parents may take place on some occasions e.g. school trips or due to exceptional circumstances. This may take place from UCS work mobile/smart phones only; permission must first be obtained from a SMT member prior to texting a pupil.

Employees must not be friends/contacts with pupils, ex-pupils under the age of 18, or parents on Social Network or microblogging sites (e.g. Facebook) and Employees must not communicate with pupils or ex-pupils under the age of 18, and are strongly advised not to communicate with parents on these sites. Employees whose own child/children are pupils at the school should seek advice from the Headmaster.

9 Communication by Email

The Foundation's computer system contains an email facility which is intended to promote effective communication within the organisation. However, this facility should not replace face to face communication which is the Foundation's preferred method of communication particularly for discussion. Limited personal messages may be sent but these should respect the primary purpose of the email system which is for school business. This means the email system should never be used for spreading gossip, or for personal gain or in breach of any of the Foundation's standard employment policies such as sexual harassment.

Messages sent by email are to be written in accordance with the standards of any other form of written communication and the content and language used in the message must always be respectful and polite in accordance with the School's ethos. Messages should normally be directed to those individuals who need to know, copying other individuals into a message should be used for the passing on of information and out of courtesy but never to add weight to an argument. General messages to a wide group should only be issued where necessary.

Confidential information should not be sent externally by email without express authority of the Headmaster and unless the messages can be lawfully encrypted.

<u>Legal Action against the School</u>

Messages sent over the email system can give rise to legal action against the school. Claims of defamation, breach of confidentiality or contract could arise from a misuse of the system. It is therefore vital for email messages to be treated like any other form of correspondence and where necessary hard copies to be retained. Employees are also reminded that messages may be disclosed in any legal action commenced against the school relevant to the issues set out in the e-mail.

<u>The School's rights</u>

The school reserves the right to retrieve the contents of messages for the purpose of monitoring whether the use of the e-mail system is legitimate, to find lost messages or to retrieve messages lost due to computer failure, to assist in the investigations of wrongful acts, or to comply with any legal obligation.

9.1 Security of email

<u>Employees</u>

If an Employee is given access to the e-mail system they are responsible for the security of their terminal and they must not allow the terminal to be used by an unauthorised person.

An Employee should keep their personal password confidential and change it regularly. When leaving their terminal unattended or on leaving the office they should ensure that they log off the system to prevent unauthorised users using their terminal in their absence.

General Rules: Email including mobile/telephone numbers

Use of email should be primarily used for educational / school business purposes. Particular consideration should be given when emails are sent externally including to pupils and parents.

The school email address must be used for all school related-business. For the avoidance of doubt, Employees' own personal email must never be used to communicate with pupils or parents.

Should an Employee receive an email message which has been wrongfully delivered to their email address they should notify the sender by redirecting the message to that person. In the event the email message contains confidential information they must not disclose or use that confidential information. Should an Employee receive an email which contravenes this policy the email should be brought to the attention of the Headmaster.

Misuse of the email system in breach of this policy statement will be considered to be misconduct and will be dealt with within the framework of the school's disciplinary procedure.

Misuse of the email system by transmission of any material in any of the following ways may constitute gross misconduct (this list is non-exhaustive):

- Defamatory;
- Offensive or obscene;
- Untrue or malicious;
- In breach of copyright.

Pupils

Pupils are provided with access to the school's email system. They may only send email or participate in on-line conversations in class when authorised by a teacher. At all times, pupils and staff should use school email only for school-related communication. Polite and appropriate language must always be used. Emails must never be used in any way that could cause offence or harm to another individual.

10 Use of Hand-Held Technology

Employees

Employees are permitted to bring their own mobile devices into the school. They are required to use their professional judgement as to when it is appropriate to use them. Our advice is that

- Personal hand-held devices will be used in lesson time only when there is an educational reason for doing so, or in an emergency or extreme circumstances;
- Members of staff are free to use these devices outside teaching time;

- Images or videos of pupils may be created on personal hand-held devices with prior approval of the employee's relevant line-manager. The images or videos must only be created for educational purposes and must be transferred to the school's network and deleted permanently from the employees personal device as soon as reasonably practicable. Images or video of pupils must not otherwise be stored on the personal mobile devices of staff;
- School mobile phones and tablets are available for professional use by staff (for example, when engaging in off-site activities).

Pupils

Pupils in the Lower and Middle School will not be allowed access to their mobile phones or tablets during the school day from registration onwards other than at lunchtime on games afternoons unless the device is officially approved by the school for educational use. There are very clear health and social reasons why we should adopt this position. We recognise that there may be good reasons why families would want their sons to have access to a phone whilst travelling to school. However, once at school all communication during the day should be made via the school office. Pupils must not use mobile phones or tablets at any stage after the start of the school day unless instructed to do so by their subject teacher. Parents / carers should be aware that breaches of discipline or suspected breaches of discipline by a pupil may lead to the temporary confiscation of a phone or tablet by a member of staff.

Mobile devices owned by the school may be handed to pupils for use in lessons in certain departments. Rules governing the use of these are included in this Policy.

11 The use of digital resources in academic work

When using the internet for research or recreation, users must recognise that the internet cannot always be regarded as a reliable source of information.

- Users must not download and use material, or copy and paste content which is subject to copyright. Content ownership must be respected at all times. (Most sites will allow the use of published materials for educational use. Teachers and librarians will give guidelines on how and when users should use information from the Internet.)
- Where work is protected by copyright, no attempt should be made to illegally download copies (including music and videos).
- When users are accessing the internet to find information, they must take care to check that the information that they access is accurate; the work of others may not be truthful and may be a deliberate attempt to mislead.
- Downloaded material must be employed in an appropriate manner in users' work, sources listed in a bibliography and any directly quoted material clearly specified.
- In respect of coursework or any other work which is to be examined externally, pupils must keep the original work or a copy of it on the school network so as not to be solely reliant on their own laptop or desktop when accessing the material.

12 The integrity and smooth running of ICT systems

Users must respect the security and integrity of the school's ICT systems and of the technology available within school, irrespective of whether the device being used belongs to the school or to someone else.

In the interests of the smooth running of the school system and the fairness of access to the available resources:

- Users must recognise that the school network is for educational use and not use the systems for personal or recreational use unless they have permission to do so.
- Users must help keep the network available to their fellow users by refraining from time- and space-consuming downloads of large files.
- The school ICT systems should not be used for on-line gaming, on-line gambling, internet shopping, file sharing (apart from file-sharing facilities which have been set up by the school for educational or administrative purposes) or video broadcasting (e.g. YouTube), unless users have permission to do so.
- Users must accept that, if they use their own personal hand held / external devices (mobile phones /tablets/ USB etc) in school, they must follow the rules set out in this policy, in the same way as if they were using school equipment.
- All users must understand the risks and must not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor should they try to use any programs or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.
- If, when pupils are provided with a mobile device to use in class, they discover that there is material left on the device by a previous user, they must inform the subject teacher immediately.
- All users must immediately report any damage or faults involving equipment or software, however this may have happened.
- Users must not open any attachments to emails, unless they know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programs.
- Users must not install or attempt to install programs of any type on a machine, or store programs on a computer, nor should users try to alter computer settings.
- Pupils should not attempt to break into or decrypt the wireless system established by the school.
- All users should understand that if they are connected to the school's wifi, that the school will routinely monitor their activity.

13 Sanctions

Users must be aware that they are responsible for their actions, both in and out of school.

The school also has the right to take action against users if they are involved in incidents of inappropriate behaviour, that are covered in this agreement, when they are out of school and where they involve membership of the school community (examples would be cyber-bullying, racism, use of images or personal information that may be construed as offensive to another member of the school community).

Under the terms of the DfE advice "Searching, screening and confiscation" (January 2018) the school has the right to confiscate mobile phones or other electronic devices without consent or parental permission if they have reason believe that they may contain pornography or youth produced sexual images [YPSI]. Any data, files or images that are believed to be illegal must be passed to the police as soon as practicable without deleting them. Any data, files or images that are not believed to be unlawful, may be deleted or kept as evidence of a breach of the school's Behaviour and Discipline Policy.

Staff have the right to confiscate any device that they have good reason to believe may be used to cause harm, disrupt teaching, break school rules, damage property, cause personal injury or commit any other offence.

All users who fail to comply with this Policy may be subject to disciplinary action. We may undertake a more detailed investigation, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses involved. For pupils, this may include loss of access to the school network / internet, detentions or suspensions, contact with parents, expulsion (in the event of systematic or persistent cyber-bullying or abuse) and, in the event of illegal activities such as sexting or youth produced sexual imagery, involvement of the police. Pupils must understand that the school makes no distinction between bullying and cyber-bullying.

Employees guilty of misconduct will be subject to disciplinary procedures which could lead to dismissal.

If there is the suspicion or evidence that a criminal act has been committed by any user of the ICT system, they may be reported to the police and the school may provide to the police any evidence obtained from its monitoring records.

14 Online-Safety Education

The education of pupils in online safety is an important part of the school's provision. Children and young people need the help and support of the school to recognise and avoid online-safety risks and build their resilience. This is particularly important for helping children to stay safe out of school where technical support and filtering may not be available to them.

Online-Safety education is provided in the following ways:

- Online-safety is built into programmes in PSHE and other lessons and is covered both in assemblies and talks by outside speakers to both pupils and parents in the Lower and Middle Schools. This is regularly revisited, covering the use of ICT both in school and outside. Entry form PSHE deals specifically with cyberbullying, and this is taken up again in the Shell. Lower Remove PSHE deals with pornography in its Sex and Relationships programme. In both the Shell and Lower Remove issues related specifically to texting and peer on peer abuse are tackled in accordance with Keeping Children Safe in Education (September 2020).
- When developing the teaching of online safety we will have regard to the Department of Education guidance Teaching online safety in schools available at: https://www.gov.uk/government/publications/teaching-online-safety-in-schools
- Key online-safety messages are reinforced through further input via pastoral activities, as well as informal conversations when the opportunity arises.
- Pupils are directed to the Acceptable Use Agreement and there is discussion of its terms.
- Outside speakers invited to give talks to pupils and parents may also refer to aspects of online-safety.
- In lessons where internet use is pre-planned, it is best practice that pupils should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

- Where pupils are allowed to freely search the internet, staff should be vigilant in monitoring the content of the websites the young people visit, encouraging them to discuss anything of which they are unsure and implementing sanctions and/or support as necessary.

The teaching of online safety should focus on:

- how to critically evaluate and make judgements on online content
- how to recognise techniques used to persuade or manipulate, for example extremist views, grooming and targeted marketing
- what is and is not acceptable online behaviour
- identifying online risks
- how to get help and support.

Pupils should be taught all elements of online safety included in the curriculum so that they:

- use technology safely and respectfully, keeping personal information private; identify where to go for help and support when they have concerns about content or contact on the internet or other online technologies

- can evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems

- are responsible, competent, confident and creative users of information and communication technology.

Teaching online safety should enable pupils to:

- understand the specific harms and risks inherent in using the internet, for example how people can behave differently on the internet and how the internet can be used to magnify and distort information and provide a platform for "fake news" and extremist views;

- how to stay safe online, how to identify online harm and abuse and what actions to take report this.

15 Information Literacy

- Pupils should be taught in all lessons to be critically aware of the content they access online and be guided to check the accuracy of information by employing such techniques as:
    - Checking the likely validity of the URL (web address)
    - Cross-checking references
    - Checking the pedigree of the compilers / owners of the website
    - Referring to other (including non-digital) sources

- Pupils will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- Pupils are taught how to make the best use of search engines to gain the information they require.

16 Disclaimer

In common with other media such as magazines, books and video, some material available via the Internet is unsuitable for pupils. The school will take all reasonable precautions to ensure that users access only appropriate material. However, it is not possible to guarantee that Users will never come across unsuitable material while using a school networked computer. University College School will not accept liability for the material accessed, or any consequences of internet access.

Social Media Policy

1 Introduction

The widespread availability and use of social media applications bring opportunities to understand, engage and communicate in new and exciting ways. It is important that we are able to use these technologies and services effectively to extend teaching and learning at University College School. However, we must also ensure that the School balances this with our duties for safeguarding pupils and protecting the brand and image of the School. This policy sets out protocols for the use of school-sanctioned social media for educational purposes and guidelines for personal use.

2 Definitions and Scope

Social networking applications include, but are not limited to: Blogs, Online discussion forums, Collaborative spaces, Media sharing services, 'Microblogging' applications, and online gaming environments. Examples include Twitter, Facebook, Windows Live Messenger, YouTube, Flickr, Xbox Live, Blogger, TikTok, Tumblr, and comment streams on public websites such as newspaper sites. Many of the principles of this policy also apply to other types of online presence such as virtual worlds.

All members of staff should bear in mind that information they share through social networking applications, even if they are on private spaces, are still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006 and other legislation. They must also operate in line with the school's Equality, Child Protection, and Online Policies

Protocols

When using social media for educational purposes, the following practices should be observed:

- Staff should set up a distinct and dedicated social media site or account for educational purposes. This should be entirely separate from any personal social media accounts held by that member of staff, and must be linked to an official school email account.
- The URL and identity of the site should be notified to the appropriate Head of Department and the Assistant Head (Director of Partnerships and Public Engagement) before use by pupils.
- The content of any school-sanctioned social media site should be solely professional and should reflect well on the school. 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 University College School.
- The proposed audience and level of interactive engagement with the site, for example whether pupils, school staff or members of the public will be able to contribute content to the site, must be discussed with the school's Assistant Head (Director of Partnerships and Public Engagement) and Head of Department.
- Staff must be careful when publishing photographs of children. In some cases it is necessary to obtain parental permission and pupils must not be identifiable by name or by other means. Please see the UCS Child Protection and Safeguarding Policy for more details on using images of children.
- Care must be taken that any links to external sites from the account are appropriate and safe.

- Any inappropriate comments on school-sanctioned social media should immediately be removed and reported to the moderator of the site.
- When possible, all social media accounts created for educational purposes should include a link or reference to the School's website, www.ucs.org.uk. This will indicate that the site is sanctioned by University College School.
- 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.
- 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 seek to post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.
- 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 also ensure that the webspace 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.

When using social media for personal purposes, the following practices should be observed:

- Staff should not invite, accept or engage in communications with parents or pupils from the UCS community on any personal social media sites. Staff should not accept any current pupil of any age or any ex-pupil of the school under the age of 18 as a friend, follower, subscriber or similar on any personal social media account
- Staff members should reject 'friend requests' from pupils in their personal social media accounts. Staff should request pupils to only use official school sanctioned groups to communicate regarding the school.
- If any member of staff is aware of any inappropriate communications involving any child in any social media, these should be reported to the Deputy Head (Pastoral).
- All email communication between staff and members of the school community on school business must be made from an official school email account.
- Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can to protect their own privacy. Staff members should also avoid posting home addresses, telephone numbers and other personal information and should consider using an alternative email address.
- Staff are advised to avoid posts or comments that refer to specific matters related to the school and members of its community on any social media accounts and should consider the reputation of UCS in any posts or comments made online.
- When staff wish to engage in social media to comment or add to a professional discussion as an employee of University College School, they should state that all opinions expressed are their own and do not reflect those of University College School.

The following procedures should be followed before creating a new social media site:

- University College School social media sites can be created only by or on behalf of the school. Site administrators and moderators must be UCS employees or other authorised people.
- Approval for creation of sites for work purposes, whether hosted by the school or hosted by a third party such as a social networking site, must be obtained from the staff

member's Head of Department/line manager and the school's Assistant Head (Director of Partnerships and Public Engagement). Approval for participating, on behalf of University College School, on sites created by staff members or third parties must be obtained from the staff member's Head of Department/line manager and the Assistant Head (Director of Partnerships and Public Engagement).

- The school's Assistant Head (Director of Partnerships and Public Engagement) must be consulted about the purpose of the proposed site and its content and approval must be obtained for the use of the school logo and brand. Areas to discuss: aims, audience, contributors, content and moderators.