

**Online Safety Policy**

Agreed October 2018

Review Date October 2019

**Development / Monitoring / Review of this Policy**

4

This Online Safety policy has been developed in collaboration with.

DSL for Child Protection/Safeguarding

Members of SLT

Online Safety Coordinator

Staff – including teachers, support staff, technical staff

Governors

Student Voice

Consultation with the whole college community has taken place through a range of formal and informal meetings.

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This Online Safety policy was approved by the *Governing Body*  |  |
| The implementation of this Online Safety policy will be monitored by the: | *DSL – Alison Hodgson**College Governors**SLT* |
| Monitoring will take place at regular intervals: | *At least once a year* |
| The *Governing Body*  will receive a report on the implementation of the Online Safety policy generated by the monitoring group (which will include anonymous details of Online Safety incidents) at regular intervals: | *At least once a year* |
| The Online Safety Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to Online Safety or incidents that have taken place. The next anticipated review date will be: | *October 2019* |
| Should serious Online Safety incidents take place, the following external persons / agencies should be informed: | *LA/BTLS (British Telecommunications Lancashire Services), LA Safeguarding Officer, Police*  |

The college will monitor the impact of the policy using:

• Logs of reported incidents

• Monitoring logs of internet activity (including sites visited)/filtering

• Internal monitoring data for network activity

• Surveys / questionnaires of:

• students

• parents / carers evaluation forms

• staff

6

**Scope of the Policy**

This policy applies to all members of the collegecommunity (including staff, students, volunteers, parents / carers, visitors) who have access to and are users of college ICT systems, both in and out of the college.

The Education and Inspections Act 2006 empowers Headteachers to such extent as is reasonable, to regulate the behaviour of students when they are off the college 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 covered by this policy, which may take place outside of the college, but is linked to membership of the college. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

The collegewill deal with such incidents within this policy and associated behaviour and anti-bullying policies and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of college.

The Unity College Online Safety Policy follows guidance available from the education department and provides a detailed summary of actions taken by the college to ensure Online Safety. It is revised annually and should be read in conjunction with our Acceptable Use Policy and with material from CEOP.

This Online Safety Policy operates in conjunction with other policies including those for Student Behaviour, Bullying, Curriculum, Data Protection, Safeguarding Children and Security, plus the Home-School Agreement.

**Roles and Responsibilities**

7

The following section outlines the Online Safety roles and responsibilities of individuals and groups within the college.

**Governors:**

Governors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy on a yearly basis. This will be carried out by the Governors receiving regular information about Online Safety incidents and monitoring reports. A member of the Governing Body has taken on the role of *Online Safety Governor* , Richard Kelly. The role of the Online Safety Governor will include:

*•* regular meetings with the Online Safety Co-ordinator

• regular monitoring of Online Safety incident logs

• regular monitoring of filtering / change control logs

*•* reporting to relevant Governors

**Headteacher and Senior Leaders:**

• The Headteacher has a duty of care for ensuring the safety (including Online Safety) of members of the college community, though the day to day responsibility for Online Safety will be delegated to the Online Safety Co-ordinator.

• The Headteacher and (at least) another member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff**.**

*•* The Headteacher and Senior Leaders are responsible for ensuring that the DSLand other relevant staff receive suitable training to enable them to carry out their Online Safety roles and to train other colleagues, as relevant.

• The Headteacher and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in college who carry out the internal Online Safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.

• The Senior Leadership Team will receive regular monitoring reports from the DSL and Online Safety Co-ordinator *.*

**Online Safety Coordinator: (DSL Child Protection/Safeguarding)**

• leads the Online Safety committee

• takes day to day responsibility for Online Safety issues and has a leading role in establishing and reviewing the college Online Safety policies / documents

• ensures that all staff are aware of the procedures that need to be followed in the event of an Online Safety incident taking place.

• provides training and advice for staff

• liaises with the Local Authority

• liaises with college technical staff

• receives reports of Online Safety incidents and creates a log of incidents to inform future Online Safety developments

• meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering / change control logs

• attends relevant meeting of Governors

• reports regularly to Senior Leadership Team

**Network Manager / Technical staff:**

Unity College has a managed ICT service provided by Chess ICT Ltd and it is our responsibility to ensure that the managed service provider maintains a secure network. The managed service provider will be made fully aware of the college Online Safety policy and procedures.

The Network Manager / Technical Staff / Co-ordinator for ICT / Computing is responsible for ensuring:

**•** that the college’s technical infrastructure is secure and is not open to misuse or malicious attack.

• that users may only access the networks and devices through a properly enforced password protection policy.

*•* the filtering policy (Cumbria and Lancashire online Network CLEO), is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person.

• that the use of the network / internet / remote access attempted misuse can be reported to the Headteacher / Senior Leader; Online Safety Coordinator for investigation / action / sanction

• that monitoring software / systems are implemented and updated as agreed in college / academy policies (lightspeed implemented).

**Teaching and Support Staff**

are responsible for ensuring that:

**•** they have an up to date awareness of Online Safety matters and of the current college Online Safety policy and practices.

• they have read, understood and signed the Staff Acceptable Use Policy / Agreement (AUP).

• they report any suspected misuse or problem to the Headteacher/SLT or Online Safety Coordinator for investigation / action / sanction.

• all digital communications with students / parents / carers should be on a professional level and only carried out using official college systems .

• Online Safety issues are embedded in all aspects of the curriculum and other activities .

• students understand and follow the Online Safety and acceptable use policies.

• students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• they monitor the use of digital technologies, mobile devices, cameras etc in lessons and other college activities (where allowed) and implement current policies with regard to these devices.

*•* in lessons, where internet use is pre-planned, students 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.

**Child Protection / Safeguarding Designated Person (DSL)**

DSL’s will be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:

• sharing of personal data

• access to illegal / inappropriate materials

• inappropriate online contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

**Online Safety Group**

The Online Safety Group provides a consultative group that has wide representation from the college community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. Depending on the size or structure of the college this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Governing Body.

Members of the Online Safety Group (or other relevant group) will assist the Online Safety Coordinator with:

• the production / review / monitoring of the college Online Safety policy / documents.

• the production / review / monitoring of the college filtering policy and requests for filtering changes.

*•* mapping andreviewing the Online Safety curricular provision – ensuring relevance, breadth and progression.

*•* monitoring network / internet / incident logs.

*•* consulting stakeholders – including parents / carers and the students about the Online Safety provision.

*•* monitoring improvement actions identified through use of the 360 degree safe self- review tool.

Students:

**•** are responsible for using the college digital technology systems in accordance with the Student Acceptable Use Policy.

• have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations.

• need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so.

• will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the taking / use of images and on cyber-bullying.

• should understand the importance of adopting good Online Safety practice when using digital technologies out of college and realise that the college’s Online Safety Policy covers their actions out of college, if related to their membership of the college.

Parents / Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet / mobile devices in an appropriate way. The college will take every opportunity to help parents understand these issues through parents’ evenings, newsletters, letters, / VLE and information about national / local Online Safety campaigns / literature*.* Parents and carers will be encouraged to support the college in promoting good Online Safety practice and to follow guidelines on the appropriate use of:

**•** digital and video images taken at college events

• access to parents’ sections of the website / VLE and online student records

• their children’s personal devices in the college

*Policy Statements*

11

Education – students

Whilst regulation and technical solutions are very important, their use must be balanced by educating students to take a responsible approach. The education of students in Online Safety is therefore an essential part of the college’s Online Safety provision. Children and young people need the help and support of the college to recognise and avoid Online Safety risks and build their resilience.

Online Safety should be a focus in all areas of the curriculum and staff should reinforce Online Safety messages across the curriculum. The Online Safety curriculum should be broad, relevant and provide progression, with opportunities for creative activities, and will be provided in the following ways:

* A planned Online Safety curriculum provided as part of Computing and ID lessons and regularly revisited
* Key Online Safety messages reinforced as part of a planned programme of assemblies and PD (Personal Development) activities
* Students taught in all lessons to be critically aware of the materials / content they access online and be guided to validate the accuracy of information.
* Students taught to acknowledge the source of information used and to respectcopyrightwhen using material accessed on the internet
* Students encouraged to adopt safe and responsible use both within and outside college
* Staff to act as good role models in their use of digital technologies, the internet and mobile devices
* Students to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
* Students will be expected to know and understand college policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand college policies on the taking/use of images and on cyber-bullying.
* Students should understand the importance of adopting good Online Safety practice when using digital technologies out of school and realise that the college’s Online Safety Policy covers their actions out of school, if related to their membership of the college.
* In lessons where internet use is pre-planned, it is best practice that students are 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 students are allowed to freely search the internet, staff will be vigilant in monitoring the content of the websites the young people visit.
* It is accepted that from time to time, for good educational reasons, students may need to research topics (eg racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that those sites are temporarily removed from the filtered list for the period of study. Any request to do so, should be auditable, with clear reasons for the need.

Education – parents / carers

Many parents and carers have only a limited understanding of Online Safety risks and issues, yet they play an essential role in the education of their children and in the monitoring / regulation of the children’s online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

The college will therefore seek to provide information and awareness to parents and carers through:

*•* Curriculum activities

• Letters, newsletters, web site, VLE

• Parents / Carers evenings / sessions

• High profile events / campaigns eg Safer Internet Day

• Reference to the relevant web sites / publications (see appendix for further links / resources)

Education & Training – Staff / Volunteers

It is essential that all staff, including volunteers, receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• Online Safety training will be made available to staff. This will be regularly updated and reinforced.

• All new staff should receive Online Safety training as part of their induction programme, ensuring that they fully understand the college Online Safety policy and Acceptable Use Agreements.

*•* The DSL will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.

• This Online Safety policy and its updates will be kept updated on the Intranet. Staff will be directed to updates.

• The DSL will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / Online Safety / health and safety / child protection by:

• Participation in college training / information sessions for staff or parents (this may include attendance at assemblies / lessons).

Technical – infrastructure / equipment, filtering and monitoring

* College technical systems will be managed in ways that ensure that the college meets
 recommended technical requirements.
* Servers, wireless systems and cabling must be securely located and physical access restricted.
* All users will have clearly defined access rights to college technical systems and devices, and will be provided with a username and secure password. Users are responsible for the security of their username and password.
* The managed Service Provider (LLICT) is responsible for ensuring that software licence logs are accurate and up to date.
* Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband via CLEO using Lightspeed managed by LCC. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes. Internet filtering will ensure that children are safe from terrorist and extremist material when accessing the internet.
* College technical staff regularly monitor and record the activity of users on the college technical systems and users are made aware of this in the Acceptable Use Agreement.
* An appropriate system is in place for users to report any actual / potential technical incident / security breach to the Online Safety co-ordinator.
* Appropriate security measures are in place through Chess ICT Ltd to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the college systems and data. The college infrastructure and individual workstations are protected by up to date virus software.
* An agreed policy is in place that allows staff to / forbids staff from downloading executable files and installing programmes on college devices.
* An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on college devices. Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured. (see College Personal Data Policy Template in the appendix for further detail)

Use of digital and video images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and students instant use of images that they have recorded themselves or downloaded from the internet. However, staff, parents / carers and students need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyber-bullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. The college will inform and educate users about these risks and will implement policies to reduce the likelihood of the potential for harm:

**•** When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet eg on social networking sites.

•In accordance with guidance from the Information Commissioner’s Office, parents / carers cannot take videos and digital images of their children at college events for their own personal use.

• Staff and volunteers are allowed to take digital / video images to support educational aims, but must follow college policies concerning the sharing, distribution and publication of those images. Those images should only be taken on college equipment, the personal equipment of staff should not be used for such purposes.

• Care should be taken when taking digital / video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the college into disrepute.

• Students must not take, use, share, publish or distribute images of others without their permission.

• Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images.

• Written permission from parents or carers will be obtained before photographs of students are published on the college website (may be covered as part of the AUA signed by parents or carers at the start of the year and their full name used).

• Student’s work can only be published with the permission of the student and parents or carers.

Data Protection

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998 and the General Data Protection Regulations which states that personal data must be:

• Fairly and lawfully processed

• Processed for limited purposes

• Adequate, relevant and not excessive

• Accurate

• Kept no longer than is necessary

• Processed in accordance with the data subject’s rights

• Secure

• Only transferred to others with adequate protection.

The college must ensure that:

* It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
* Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
* All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”**.**
* It complies with a Data Protection Policy and GDPR.
* It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
* It has clear and understood arrangements for the security, storage and transfer of personal data
* Data subjects have rights of access and there are clear procedures for this to be obtained
* There are clear and understood policies and routines for the deletion and disposal of data
* There is a policy for reporting, logging, managing and recovering from information risk incidents
* There are clear Data Protection clauses in all contracts where personal data may be passed to third parties
* There are clear policies about the use of cloud storage / cloud computing which ensure that such data storage meets the requirements laid down by the Information Commissioner’s Office.

Staff must ensure that they:

• At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

• Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.

**•** The official colleg*e* email service may be regarded as safe and secure and is monitored.Users should be aware that email communications are monitored.

• Users must immediately report, to the nominated person – in accordance with the college policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.

• Any digital communication between staff and students or parents / carers (email, chat, VLE etc) must be professional in tone and content.

*•* Students will be taught about Online Safety issues, such as the risks attached to the sharing of personal details. They will also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

• Personal information should not be posted on the college website and only official email addresses should be used to identify members of staff.

Social Media - Protecting Professional Identity

Reasonable steps to prevent predictable harm must be in place.

The college provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students,, staff and the college through limiting access to personal information:

* Training to include: acceptable use; social media risks; checking of settings; data protection; reporting issues
* Clear reporting guidance, including responsibilities, procedures and sanctions
* Risk assessment, including legal risk

College staff should ensure that:

* No reference should be made in social media to students, parents /carers or college staff.
* They do not engage in online discussion on personal matters relating to members of the college community.
* Personal opinions should not be attributed to the college or local authority.
* Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information.

The college’s use of social media for professional purposes will be checked regularly by the DSL and the Online Safety committee to ensure compliance with the Social Media, Data Protection, Communications, Digital Image and Video Policies.

Responding to incidents of misuse

Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart (below and appendix) for responding to online safety incidents and report immediately to the police.



Other Incidents

In the event of suspicion, all steps in this procedure should be followed:

* Have more than one senior member of staff. This is vital to protect individuals if accusations are subsequently reported.
* Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
* It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
* Record the url of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
* Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does then appropriate action will be required and could include the following:

• Internal response or disciplinary procedures

• Involvement by Local Authority or national / local organisation (as relevant).

• Police involvement and/or action

* If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
* incidents of ‘grooming’ behaviour
* the sending of obscene materials to a child
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials
* Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

It is important that all of the above steps are taken as they will provide an evidence trail for the college and possibly the police and demonstrate that visits to these sites were carried out for child protection purposes. The completed form should be retained by the group for evidence and reference purposes.

22

Appendices

Unity College Internet & E-Mail Acceptable use Policy

LCC Guidance on the Use of Social Networking Sites and other forms of Social Media

Student / Pupil Acceptable Use Agreement template (older children)

Staff and Volunteers Acceptable Use Agreement Policy template

Online Safety Committee Terms of Reference

Responding to incidents of misuse – flowchart

Record of reviewing sites (for internet misuse)

College Reporting Log template

College Training Needs Audit template

College Technical Security Policy template

College Online Safety Committee Terms of Reference

Glossary of terms

24

APPENDICES

Student Acceptable Use Agreement

College Policy

Digital technologies have become integral to the lives of children and young people, both within colleges and outside college. These 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. Young people should have an entitlement to safe internet access at all times.

**This Acceptable Use Policy is intended to ensure:**

• that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.

• that college systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

The college will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use college ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users.

**For my own personal safety:**

• I understand that the collegewill monitor my use of the systems, devices and digital communications.

• I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will be aware of “stranger danger”, when I am communicating online.

• I will not disclose or share personal information about myself or others when online (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )

• If I arrange to meet people off-line that I have communicated with online, I will do so in a public place and take an adult with me.

• I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online.

**I understand that everyone has equal rights to use technology as a resource and:**

• I understand that the college systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not use the college systems or devices for online gaming, online gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

25

**I will act as I expect others to act toward me:**

• I will respect others’ work and property and will not access, copy, remove or otherwise alter any other user’s files, without the owner’s knowledge and permission.

• I will be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will not take or distribute images of anyone without their permission.

**I recognise that the college has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the college:**

• I will only use my own personal devices (mobile phones / USB devices etc) in college if I have permission I understand that, if I do use my own devices in the college, I will follow the rules set out in the relevant policies and in this agreement, in the same way as if I was using college equipment.

• I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

• I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will not install or attempt to install or store programmes of any type on any college device, nor will I try to alter computer settings.

• I will only use social media sites with permission and at the times that are

**When using the internet for research or recreation, I recognise that:**

• I should ensure that I have permission to use the original work of others in my own work

• Where work is protected by copyright, I will not try to download copies (including music and videos)

• When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

**I understand that I am responsible for my actions, both in and out of college:**

• I understand that the collegealso has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of college and where they involve my membership of the college community (examples would be cyber-bullying, use of images or personal information).

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the college network / internet, consequences outlined in the behaviour policy and in the event of illegal activities involvement of the police.

**Please complete the sections on the next page to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to college systems and devices.**

Student Acceptable Use Agreement Form

This form relates to the student Acceptable Use Agreement, to which it is attached.

Please complete the sections below to show that you have read, understood and agree to the rules included in the Acceptable Use Agreement. If you do not sign and return this agreement, access will not be granted to college ICT systems.

I have read and understand the above and agree to follow these guidelines when:

• I use the college systems and devices (both in and out of college)

• I use my own devices in the college(when allowed) eg mobile phones, gaming devices USB devices, cameras etc

• I use my own equipment out of the college / academy in a way that is related to me being a member of this college eg communicating with other members of the college, accessing college email, VLE, website etc.

Name of Student

Group /PD

Signed

Date

Parent / Carer Counter signature (optional)

|  |
| --- |
|  |

Use Agreement

Digital technologies have become integral to the lives of children and young people, both within colleges and outside college. These technologies provide powerful tools, which open up new opportunities for everyone. They can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that college systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their online behaviour.

The college will try to ensure that students will have good access to digital technologies to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the college expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the college in this important aspect of the college’s work.

Permission Form

Parent / Carers Name Student Name

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at college.

Use of Digital / Video Images

The use of digital / video images plays an important part in learning activities. Students / Pupils and members of staff may use digital cameras to record evidence of activities in lessons and out of college. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the college website and occasionally in the public media,

The college will comply with the Data Protection Act and request parents / carers permission before taking images of members of the college. We will also ensure that when images are published that the young people cannot be identified by the use of their names.

Parents / carers are requested to sign the permission form below to allow the college to take and use images of their children and for the parents / carers to agree

Digital / Video Images Permission Form

Parent / Carers Name

Student Name

As the parent / carer of the above student, I agree to the college taking and using digital / video images of my child / children. I understand that the images will only be used to support learning activities or in publicity that reasonably celebrates success and promotes the work of the college.

Yes / No

Yes / No

I agree that if I take digital or video images at, or of, – college events which include images of children, other than my own, I will abide by these guidelines in my use of these images.

Signed

Date

Use of Biometric Systems

The college uses biometric systems for the recognition of individual children for a cashless canteen system.

Biometric technologies have certain advantages over other automatic identification systems as pupils do not need to remember to bring anything with them (to the canteen or college library) so nothing can be lost, such as a swipe card.

The college has carried out a privacy impact assessment and is confident that the use of such technologies is effective and justified in a college context.

No complete images of fingerprints / palms are stored and the original image cannot be reconstructed from the data. That is, it is not possible for example, to recreate a student's fingerprint or even the image of a fingerprint from what is in effect a string of numbers.

Parents / carers are asked for permission for these biometric technologies to be used by their child:

Parent / Carers Name

Staff (and Volunteer) Acceptable Use Policy Agreement

College Policy

New technologies have become integral to the lives of children and young people in today’s society, both within colleges / academies and in their lives outside college. 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. They also bring opportunities for staff to be more creative and productive in their work. All users should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

• that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.

• that college ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

• that staff are protected from potential risk in their use of ICT in their everyday work.

The college will try to ensure that staff and volunteers will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use college ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students / pupils receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed Online Safety in my work with young people.

For my professional and personal safety:

• I understand that the collegewill monitor my use of the ICT systems, email and other digital communications.

• I understand that the rules set out in this agreement also apply to use of college ICT systems (eg laptops, email, VLE etc) out of college, and to the transfer of personal data (digital or paper based) out of college.

• I understand that the college ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the college. (colleges should amend this section in the light of their policies which relate to the personal use, by staff and volunteers, of college systems)

• I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.

• I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.

28

I will be professional in my communications and actions when using college ICT systems:

• I will not access, copy, remove or otherwise alter any other user’s files, without their express permission.

• I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.

• I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the college’s policy on the use of digital / video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg on the college website / VLE) it will not be possible to identify by name, or other personal information, those who are featured.

• I will only use chat and social networking sites in college in accordance with the college’s policies. (colleges should amend this section to take account of their policy on access to social networking and similar sites)

• I will only communicate with students and parents / carers using official college systems. Any such communication will be professional in tone and manner. (colleges should amend this section to take account of their policy on communications with students and parents / carers. Staff should be made aware of the risks attached to using their personal email addresses / mobile phones / social networking sites for such communications)

• I will not engage in any online activity that may compromise my professional responsibilities.

The college and the local authority have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the college:

• When I use my mobile devices (PDAs / laptops / mobile phones / USB devices etc) in college, I will follow the rules set out in this agreement, in the same way as if I was using college equipment. I will also follow any additional rules set by the college about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses

• I will not use personal email addresses on the college ICT systems.

• I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)

• I will ensure that my data is regularly backed up, in accordance with relevant college policies.

• I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.

• I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.

• I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in college policies. (colleges should amend this section in the light of their policies on installing programmes / altering settings)

• I will not disable or cause any damage to college equipment, or the equipment belonging to others.

• I will only transport, hold, disclose or share personal information about myself or others, as outlined in the College / LA Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.

• I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by college policy to disclose such information to an appropriate authority.

• I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the internet in my professional capacity or for college sanctioned personal use:

• I will ensure that I have permission to use the original work of others in my own work.

• Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the college:

• I understand that this Acceptable Use Policy applies not only to my work and use of college ICT equipment in college, but also applies to my use of college ICT systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the college.

• I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

I have read and understand the above and agree to use the college ICT systems (both in and out of college) and my own devices (in college and when carrying out communications related to the college) within these guidelines.

Staff / Volunteer Name

Signed

Date

**Record of reviewing devices / internet sites (responding to incidents of misuse)**

|  |  |
| --- | --- |
| Group |  |
| Date |  |
| Reason for investigation |  |

**Details of first reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

**Details of second reviewing person**

|  |  |
| --- | --- |
| Name |  |
| Position |  |
| Signature |  |

Name and location of computer used for review (for web sites)

|  |
| --- |
|  |

**Web site(s) address / device Reason for concern**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Conclusion and Action proposed or taken**

|  |  |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

**Template Reporting Log**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Reporting LogGroup .............................................................. | Signature |  |  |  |  |  |  |  |  |
| Incident Reported by |  |  |  |  |  |  |  |  |
| Action taken | By whom? |  |  |  |  |  |  |  |  |
| What? |  |  |  |  |  |  |  |  |
| Incident |  |  |  |  |  |  |  |  |
| Time |  |  |  |  |  |  |  |  |
| Date |  |  |  |  |  |  |  |  |

**Training Needs Audit**

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Training Needs Audit LogGroup .............................................................. Date ................................ | Review date |  |  |  |  |  |  |  |  |
| Cost |  |  |  |  |  |  |  |  |
| To be met by: |  |  |  |  |  |  |  |  |
| Identified training need |  |  |  |  |  |  |  |  |
| Relevant trainingin last 12 months |  |  |  |  |  |  |  |  |
| Position |  |  |  |  |  |  |  |  |
| Name |  |  |  |  |  |  |  |  |

College Technical Security Policy (including filtering and passwords) - amended March 2015

Technical Security

Policy statements

The college will be responsible for ensuring that the college infrastructure / network is as safe and secure as is reasonably possible and that policies and procedures approved within this policy are implemented. It will also need to ensure that the relevant people will receive guidance and training and will be effective in carrying out their responsibilities:

**•** College technical systems will be managed in ways that ensure that the college meets recommended technical requirements.

• There will be regular reviews and audits of the safety and security of college technical systems

• Servers, wireless systems and cabling must be securely located and physical access restricted.

• Appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, work stations, mobile devices etc from accidental or malicious attempts which might threaten the security of the college systems and data.

• Responsibilities for the management of technical security are clearly assigned to appropriate and well trained staff.

• All users will have clearly defined access rights to college technical systems**.**

*•* Users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.

*•* PPA/ARA is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations

*•* Mobile device security and management procedures are in place.

• College / academy technical staff regularly monitor and record the activity of users on the college technical systems and users are made aware of this in the Acceptable Use Agreement.

• Remote management tools are used by staff to control workstations and view users activity.

• An appropriate system is in place (ABUTAR) for users to report any actual / potential technical incident to the Online Safety Coordinator / Network Manager / Technician.

• An agreed policy is in place (to be described) for the provision of temporary access of “guests” (eg trainee teachers, supply teachers, visitors) onto the college system.

• An agreed policy is in place regarding the downloading of executable files and the installation of programmes on college devices by users.

*•* An agreed policy is in place regarding the extent of personal use that users (staff / students / pupils / community users) and their family members are allowed on college devices that may be used out of college.

• An agreed policy is in place regarding the use of removable media (eg memory sticks / CDs / DVDs) by users on college devices.

• The college infrastructure and individual workstations are protected by up to date software to protect against malicious threats from viruses, worms, trojans etc.

• Personal data cannot be sent over the internet or taken off the college site unless safely encrypted or otherwise secured.

Password Security

Policy Statements

* All users will have clearly defined access rights to college technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the Online Safety Committee.
	+ All college networks and systems will be protected by secure passwords that are regularly changed.
	+ The “master / administrator” passwords for the college systems, used by the technical staff must also be available to the Headteacher or other nominated senior leader and kept in a secure place eg college safe. Consideration should also be given to using two factor authentication for such accounts.
* Passwords for new users, and replacement passwords for existing users will be allocated by PPA.
* All users (adults and young people) will have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
* Users will change their passwords at regular intervals – as described in the staff and student sections below
* requests for password changes should be authenticated by PPA to ensure that the new password can only be passed to the genuine user.

**Staff passwords:**

* All staff users will be provided with a username and passwordby PPA who will keep an up to date record of users and their usernames.

Student passwords

* **All users** **will be provided with a username and password** by PPAwho will keep an up to date record of users and their usernames.

Training / Awareness

It is essential that users should be made aware of the need for keeping passwords secure, and the risks attached to unauthorised access / data loss. This should apply to even the youngest of users, even if class log-ons are being used.

Members of staff will be made aware of the college’s password policy:

• at induction

• through the college’s Online Safety policy and password security policy

• through the Acceptable Use Agreement

Sstudents will be made aware of the college’s password policy:

• in lessons

• through the Acceptable Use Agreement

Audit / Monitoring / Reporting / Review

The responsible person (PPA) will ensure that full records are kept of:

• User Ids and requests for password changes

Filtering

36

Responsibilities

The responsibility for the management of the college’s filtering policy will be held by Chess ICT Ltd PPA/ARA. They will manage the college filtering, in line with this policy and will keep records / logs of changes and of breaches of the filtering systems.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the college filtering service will:

**•** be logged in change control logs

• be reported to a second responsible person ARA/PPA:

All users have a responsibility to report immediately to (PPA) any infringements of the college’s filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programmes or software that might allow them to bypass the filtering / security systems in place to prevent access to such materials.

Policy Statements

Internet access is filtered for all users. Differentiated internet access is available for staff and customised filtering changes are managed by the college. Illegal content is filtered by broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list and other illegal content lists . Filter content lists are regularly updated and internet use is logged and frequently monitored. The monitoring process alerts the college to breaches of the filtering policy, which are then acted upon. There is a clear route for reporting and managing changes to the filtering system. Where personal mobile devices are allowed internet access through the college network, filtering will be applied that is consistent with college practice.

* The college maintains and supports the managed filtering service provided by the Internet Service Provider (or other filtering service provider)

• Mobile devices that access the college internet connection will be subject to the same filtering standards as other devices on the college systems

• Any filtering issues should be reported immediately to the filtering provider.

• Requests from staff for sites to be removed from the filtered list will be considered by the technical staff / Chess ICT Ltd.

Education / Training / Awareness

Students will be made aware of the importance of filtering systems through the Online Safety education programme. They will also be warned of the consequences of attempting to subvert the filtering system.

Staff users will be made aware of the filtering systems through:

• the Acceptable Use Agreement

• induction training

• staff meetings, briefings, Inset.

Parents will be informed of the college’s filtering policy through the Acceptable Use Agreement and through Online Safety awareness on the VLE and other events/published material.

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The college will therefore monitor the activities of users on the college network and on college equipment as indicated in the College Online Safety Policy and the Acceptable Use Agreement.

Audit / Reporting

Logs of filtering change controls and of filtering incidents will be made available to:

• the second responsible person PPA/ARA

• Online Safety Group

• Online Safety Governor

• External Filtering provider / Local Authority / Police on request

The filtering policy will be reviewed in the response to the evidence provided by the audit logs of the suitability of the current provision

College Personal Data Handling Policy

Introduction

Colleges and their employees should do everything within their power to ensure the safety and security of any material of a personal or sensitive nature

It is the responsibility of all members of the college community to take care when handling, using or transferring personal data that it cannot be accessed by anyone who does not:

• have permission to access that data, and/or

• need to have access to that data.

Data breaches can have serious effects on individuals and / or institutions concerned, can bring the college into disrepute and may well result in disciplinary action, criminal prosecution and fines imposed by the Information Commissioners Office ~~.~~ for the college and the individuals involved. Particularly, all transfer of data is subject to risk of loss or contamination.

Anyone who has access to personal data must know, understand and adhere to this policy, which brings together the legal requirements contained in relevant data protection legislation and relevant regulations and guidance (where relevant from the Local Authority).

38

Policy Statements

The college will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.

Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.

All personal data will be fairly obtained in accordance with the “Privacy Notice” and lawfully processed in accordance with the “Conditions for Processing”.

Personal Data

The college and individuals will have access to a wide range of personal information and data. The data may be held in a digital format or on paper records. Personal data is defined as any combination of data items that identifies an individual and provides specific information about them, their families or circumstances. This will include:

• Personal information about members of the college community – including students,
 members of staff and parents / carers eg, names, addresses, contact details, legal guardianship
 contact details, health records, disciplinary records

• Curricular / academic data eg, class lists, student progress records, reports, references

• Professional records eg, employment history, taxation and national insurance records, appraisal
 records and references

• Any other information that might be disclosed by parents / carers or by other agencies working
 with families or staff members.

Responsibilities

The college’s DSL (ARA/Chess ICT Ltd) .This person will keep up to date with current legislation and guidance and will:

• determine and take responsibility for the college’s information risk policy and risk assessment

• appoint the Information Asset Owners (IAOs)

The college will identify Information Asset Owners (IAOs) for the various types of data being held (eg pupil / student information / staff information / assessment data etc). The IAOs will manage and address risks to the information and will understand:

• what information is held, for how long and for what purpose,

• how information has been amended or added to over time, and

• who has access to protected data and why.

Everyone in the college has the responsibility of handling protected or sensitive data in a safe and secure manner.

Governors are required to comply fully with this policy in the event that they have access to personal data, when engaged in their role as a Governor.

Registration

The college is registered as a Data Controller on the Data Protection Register held by the Information Commissioner.

Information to Parents / Carers – the “Privacy Notice”

In order to comply with the fair processing requirements of the DPA, the college will inform parents / carers of all students of the data they collect, process and hold on the students, the purposes for which the data is held and the third parties (eg LA, DfE, etc) to whom it may be passed. This privacy notice will be passed to parents / carers through the VLE. Parents / carers of young people who are new to the college will be provided with the privacy notice.

Training & awareness

All staff will receive data handling awareness / data protection training and will be made aware of their responsibilities, as described in this policy through:

* Induction training for new staff
* Intranet
* Staff meetings / briefings / Inset
* Day to day support and guidance from Information Asset Owners (PPA/AWH)

Risk Assessments

Information risk assessments will be carried out by managed service Chess ICT Ltd to establish the security measures already in place and whether they are the most appropriate and cost effective. The risk assessment will involve:

* Recognising the risks that are present;
* Judging the level of the risks (both the likelihood and consequences); and
* Prioritising the risks.

Secure Storage of and access to data

The college will ensure that ICT systems are set up so that the existence of protected files is hidden from unauthorised users and that users will be assigned a clearance that will determine which files are accessible to them. Access to protected data will be controlled according to the role of the user. Members of staff will not, as a matter of course, be granted access to the whole management information system.

Appendix - DfE Guidance on the wording of the Privacy Notice

Privacy Notice - Data Protection Act 1998

Unity College is a Data Controller for the purposes of the Data Protection Act. We collect information from you, and may receive information about you from your previous school and the Learning Records Service. We hold this personal data and use it to:

• support your teaching and learning;

• monitor and report on your progress;

• provide appropriate pastoral care;

• help and improve your health and wellbeing, and

• assess how well your school is doing.

This information includes your contact details, national curriculum assessment results, attendance information **1**, and personal characteristics such as your ethnic group, any special educational needs and relevant medical information. If you are enrolling for post 14 qualifications we will be provided with your unique learner number (ULN) by the Learning Records Service, and may also obtain from them details of any learning or qualifications you have undertaken.

**The college will not give information about students to anyone outside the school without their consent unless the law and our rules allow us to.**

The college are required by law to pass some information about students to the Local Authority (LA), and the Department for Education (DfE).

Any copies of information held by college re students can be accessed by contacting Unity College.

More information about how the LA and/or DfE store and use information, can be noted in the following documents:

• **What the LA does with Pupil and School Workforce data**

• **What the DfE does with Pupil data**

• **Who the DfE passes Pupil data to**

If you need any further clarification, please contact the LA or the DfE as follows:

• Stephen Clark – Information Unit Manager – 01772-531317

• Public Communications Unit **Department for Education** Sanctuary Buildings Great Smith Street, London SW1P 3BT

Website: **www.education.gov.uk**

Email: **http://www.education.gov.uk/help/contactus** Telephone: 0370 000 2288.

**In addition for Secondary and Middle deemed Secondary Colleges**

Once students are aged 13 or over, we are required by law to pass on certain information to providers of youth support services in our area. This is the local authority support service for young people aged 13 to 19 in England. We must provide both student and parent’s/s’ name(s) and address, and any further information relevant to the support services’ role. However, if students are over 16 they can ask that no information beyond names, address and date of birth be passed to the support service. Mr A Rahman will need to be informedif youwish to opt-out of this arrangement. For more information about young peoples’ services, please go to the Directgov Young People page at [www.direct.gov.uk/en/YoungPeople/index.htm](http://www.direct.gov.uk/en/YoungPeople/index.htm) or the LA website shown above.

**We will not give information about students to anyone outside the college without consent unless the law and our rules allow us to.**

We are required by law to pass some information about students to the Local Authority and the Department for Education (DfE)

If you require more information about how the Local Authority (LA) and/or DfE store and use information, then please go to the following websites:

<http://www.education.gov.uk/researchandstatistics/datatdatam/b00212337/datause>

If you are unable to access these websites we can send you a copy of this information. Please contact the LA or DfE as follows:

Public Communications Unit, Department for Education
Sanctuary Buildings, Great Smith Street, London
SW1P 3BT

Website: [www.education.gov.uk](http://www.education.gov.uk)

email: <http://www.education.gov.uk/help/contactus>
Telephone: 0370 000 2288

Electronic Devices - Searching & Deletion

Introduction

The changing face of information technologies and ever increasing student use of these technologies has meant that the Education Acts have had to change in an attempt to keep pace. Within Part 2 of the Education Act 2011 (Discipline) there have been changes to the powers afforded to colleges by statute to search pupils in order to maintain discipline and ensure safety. Colleges are required to ensure they have updated policies which take these changes into account. No such policy can on its own guarantee that the college will not face legal challenge, but having a robust policy which takes account of the Act and applying it in practice will however help to provide the college with justification for what it does.

The particular changes we deal with here are the added power to search for items ‘banned under the college rules’ and the power to ‘delete data’ stored on seized electronic devices.

Items banned under the college rules are determined and publicised by the Headteacher (section 89 Education and Inspections Act 1996).

An item banned by the college rules may only be searched for under these new powers if it has been identified in the college rules as an item that can be searched for. It is therefore important that there is a college policy which sets out clearly and unambiguously the items which:

* are banned under the college rules; and
* are banned AND can be searched for by authorised college staff

The act allows authorised persons to examine data on electronic devices if they think there is a good reason to do so. In determining a ‘good reason’ to examine or erase the data or files the authorised staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or could break the college rules.

Following an examination, if the person has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so.

The Headteacher must publicise the college behaviour policy, in writing, to staff, parents / carers and students at least once a year. (There should therefore be clear links between the search etc. policy and the behaviour policy).

Relevant legislation:

* Education Act 1996
* Education and Inspections Act 2006
* Education Act 2011 Part 2 (Discipline)
* The College Behaviour (Determination and Publicising of Measures in Academies) Regulations 2012
* Health and Safety at Work etc. Act 1974
* Obscene Publications Act 1959
* Children Act 1989
* Human Rights Act 1998
* Computer Misuse Act 1990
* Keeping Children Safe In Education (Sept 2018)
* Working together to safeguard and promote the welfare of children (July 2018)

Responsibilities

The Headteacher is responsible for ensuring that the college policies reflect the requirements contained within the relevant legislation. The formulation of these policies may be delegated to other individuals or groups. The policies will normally be taken to Governors for approval. The Headteacher will need to authorise those staff who are allowed to carry out searches.

This policy has been written by and will be reviewed by: SLT

The Headteacher has authorised the following members of staff to carry out searches for and of electronic devices and the deletion of data / files on those devices: SLT, Behaviour and Support Team.

The Headteacher may authorise other staff members in writing in advance of any search they may undertake, subject to appropriate training.

Training / Awareness

It is essential that all staff should be made aware of and should implement the college’s policy.

Members of staff should be made aware of the college’s policy on "Electronic devices – searching and deletion":

• at induction

• at regular updating sessions on the college’s Online Safety policy

Members of staff authorised by the Headteacher to carry out searches for and of electronic devices and to access and delete data / files from those devices should receive training that is specific and relevant to this role.

Specific training is required for those staff who may need to judge whether material that is accessed is inappropriate or illegal.

35

Policy Statements

Search:

The college Behaviour Policy refers to the policy regarding searches with and without consent for the wide range of items covered within the Education Act 2011 and lists those items. This policy refers only to the searching for and of electronic devices and the deletion of data / files on those devices.

Students are allowed to bring mobile phones or other personal electronic devices to college and use them only within the rules laid down by the college.

If pupils / students breach these roles:

The sanctions for breaking these rules can be found in the Behaviour Policy

Authorised staff have the right to search for such electronic devices where they reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules.

* Searching with consent - Authorised staff may search with the pupil’s consent for any item.
* Searching without consent - Authorised staff may only search without the student’s consent for anything which is either ‘prohibited’ (as defined in Section 550AA of the Education Act 1996) or appears in the college rules as an item which is banned and may be searched for.

**In carrying out the search:**

The authorised member of staff must have reasonable grounds for suspecting that a student is in possession of a prohibited item i.e. an item banned by the college rules and which can be searched for.

The authorised member of staff should take reasonable steps to check the ownership of the mobile phone / personal electronic device before carrying out a search

The authorised member of staff should take care that, where possible, searches should not take place in public places eg an occupied classroom, which might be considered as exploiting the student being searched.

The authorised member of staff carrying out the search must be the same gender as the individual being searched; and there must be a witness (also a staff member) and, if at all possible, they too should be the same gender as the student being searched.

There is a limited exception to this rule: authorised staff can carry out a search of a student of the opposite gender including without a witness present, but only where you reasonably believe that there is a risk that serious harm will be caused to a person if you do not conduct the search immediately and where it is not reasonably practicable to summon another member of staff.

Extent of the search:

The person conducting the search may not require the student to remove any clothing other than outer clothing.

The power to search without consent enables a personal search, involving removal of outer clothing and searching of pockets; but not an intimate search going further than that, which only a person with more extensive powers (e.g. a police officer) can do.

Use of Force – force cannot be used to search without consent for items banned under the college rules regardless of whether the rules say an item can be searched for.

Electronic devices

An authorised member of staff finding an electronic device may access and examine any data or files on the device if they think there is a good reason to do so (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules).

The examination of the data / files on the device should go only as far as is reasonably necessary to establish the facts of the incident. Any further intrusive examination of personal data may leave the college open to legal challenge. It is important that authorised staff should have training and sufficient knowledge of electronic devices and data storage.

If inappropriate material is found on the device it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a criminal offence or a breach of college discipline) or whether the material is of such seriousness that it requires the involvement of the police. Examples of illegal activity would include:

* child sexual abuse images (including images of one child held by another child)
* adult material which potentially breaches the Obscene Publications Act
* criminally racist material
* other criminal conduct, activity or materials

Members of staff may require support in judging whether the material is inappropriate or illegal. One or more Senior Leaders should receive additional training to assist with these decisions. Care should be taken not to delete material that might be required in a potential criminal investigation.

The college should also consider their duty of care responsibility in relation to those staff who may access disturbing images or other inappropriate material whilst undertaking a search. Seeing such material can be most upsetting. There should be arrangements in place to support such staff.

Deletion of Data

Following an examination of an electronic device, if the authorised member of staff has decided to return the device to the owner, or to retain or dispose of it, they may erase any data or files, if they think there is a good reason to do so. (i.e. the staff member must reasonably suspect that the data or file on the device in question has been, or could be, used to cause harm, to disrupt teaching or break the college rules).

If inappropriate material is found on the device, it is up to the authorised member of staff to decide whether they should delete that material, retain it as evidence (of a possible criminal offence or a breach of college discipline) or whether the material is of such seriousness that it requires the involvement of the police. A record should be kept of the reasons for the deletion of data / files.

Care of Confiscated Devices

College staff are reminded of the need to ensure the safe keeping of confiscated devices, to avoid the risk of compensation claims for damage / loss of such devices (particularly given the possible high value of some of these devices). Mobile Phone Policy assists with this. The college safe must be used to keep devices.

Audit / Monitoring / Reporting / Review

The DSL will ensure that full records are kept of incidents involving the searching for and of mobile phones and electronic devices and the deletion of data / files.

These records will be reviewed by at regular intervals. This policy will be reviewed by the Headteacher and governors annually and in response to changes in guidance

College Policy - Online Safety Committee Terms of Reference

**1. PURPOSE**

To provide a consultative group that has wide representation from the college community, with responsibility for issues regarding Online Safety and the monitoring the Online Safety policy including the impact of initiatives. Depending on the size or structure of the college this committee may be part of the safeguarding group. The group will also be responsible for regular reporting to the Full Governing Body.

**2. MEMBERSHIP**

2.1 The Online Safety committee will seek to include representation from all stakeholders.

The composition of the group should include:

* SLT member/s
* DSL
* Teaching staff member
* Support staff member
* Governor
* ICT Technical Support staff
* Student / representation (where appropriate)

2.2 Other people may be invited to attend the meetings at the request of the Chairperson on behalf of the committee to provide advice and assistance where necessary.

2.3 Committee members must declare a conflict of interest if any incidents being discussed directly involve themselves or members of their families.

2.4 Committee members must be aware that many issues discussed by this group could be of a sensitive or confidential nature

2.5 When individual members feel uncomfortable about what is being discussed they should be allowed to leave the meeting with steps being made by the other members to allow for these sensitivities.

**3. CHAIRPERSON**

The Committee should select a suitable Chairperson from within the group. Their responsibilities include:

* Scheduling meetings and notifying committee members;
* Inviting other people to attend meetings when required by the committee;
* Guiding the meeting according to the agenda and time available;
* Ensuring all discussion items end with a decision, action or definite outcome;
* Making sure that notes are taken at the meetings and that these with any action points are distributed as necessary

**4. DURATION OF MEETINGS**

Meetings shall be held termly. A special or extraordinary meeting may be called when and if deemed necessary.

**5. FUNCTIONS**

These are to assist the Online Safety Coordinator with the following:

* To keep up to date with new developments in the area of Online Safety
* To annually review and develop the Online Safety policy in line with new technologies and incidents
* To monitor the delivery and impact of the Online Safety policy
* To monitor the log of reported Online Safety incidents (anonymous) to inform future areas of teaching / learning / training.
* To co-ordinate consultation with the whole college community to ensure stakeholders are up to date with information, training and/or developments in the area of Online Safety.:
	+ Staff meetings
	+ Student / pupil forums (for advice and feedback)
	+ Governors meetings
	+ Surveys/questionnaires for students / pupils, parents / carers and staff
	+ Parents evenings
	+ Website/VLE/Newsletters
	+ Online Safety events
	+ Internet Safety Day (annually held on the second Tuesday in February)
	+ Other methods
* To ensure that monitoring is carried out of Internet sites used across the college
* To monitor filtering / change control logs (e.g. requests for blocking / unblocking sites).
* To monitor the safe use of data across the college
* To monitor incidents involving cyberbullying for staff and pupils

**6. AMENDMENTS**

The terms of reference shall be reviewed annually from the date of approval. They may be altered to meet the current needs of all committee members, by agreement of the majority

The above Terms of Reference for Unity College have been agreed

Signed by (SLT):

Date:

Date for review:

**Acknowledgement**

This template terms of reference document is based on one provided to colleges by Somerset County Council

Legislation

Colleges should be aware of the legislative framework under which this Online Safety Policy template and guidance has been produced. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

It is recommended that legal advice is sought in the advent of an e safety issue or situation.

Computer Misuse Act 1990

This Act makes it an offence to:

• Erase or amend data or programs without authority;

• Obtain unauthorised access to a computer;

• “Eavesdrop” on a computer;

• Make unauthorised use of computer time or facilities;

• Maliciously corrupt or erase data or programs;

• Deny access to authorised users.

Data Protection Act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that person data must be:

• Fairly and lawfully processed.

• Processed for limited purposes.

• Adequate, relevant and not excessive.

• Accurate.

• Not kept longer than necessary.

• Processed in accordance with the data subject’s rights.

• Secure.

• Not transferred to other countries without adequate protection.

Freedom of Information Act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications Act 2003

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

Malicious Communications Act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of Investigatory Powers Act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

• Establish the facts;

• Ascertain compliance with regulatory or self-regulatory practices or procedures;

• Demonstrate standards, which are or ought to be achieved by persons using the system;

• Investigate or detect unauthorised use of the communications system;

• Prevent or detect crime or in the interests of national security;

• Ensure the effective operation of the system.

• Monitoring but not recording is also permissible in order to:

• Ascertain whether the communication is business or personal;

• Protect or support help line staff.

• The college reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks Act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, Designs and Patents Act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications Act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal Justice & Public Order Act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they:

• Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

• Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and Religious Hatred Act 2006

This Act makes it a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Protection from Harrassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other. A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

Protection of Children Act 1978

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is a anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public Order Act 1986

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence. Children, Families and Education Directorate page 38 April 2007.

Obscene Publications Act 1959 and 1964

Publishing an “obscene” article is a criminal offence. Publishing includes electronic transmission.

Human Rights Act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of “higher law”, affecting all other laws. In the college context, human rights to be aware of include:

• The right to a fair trial

• The right to respect for private and family life, home and correspondence

• Freedom of thought, conscience and religion

• Freedom of expression

• Freedom of assembly

• Prohibition of discrimination

• The right to education

These rights are not absolute. The college is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

The Education and Inspections Act 2006

Empowers Headteachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour.

51

The Education and Inspections Act 2011

Extended the powers included in the 2006 Act and gave permission for Headteachers (and nominated staff) to search for electronic devices. It also provides powers to search for data on those devices and to delete data. (see template policy in these appendices and for DfE guidance - [http://www.education.gov.uk/colleges/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation](http://www.education.gov.uk/schools/pupilsupport/behaviour/behaviourpolicies/f0076897/screening-searching-and-confiscation)

The Protection of Freedoms Act 2012

Requires colleges to seek permission from a parent / carer to use Biometric systems

The College Information Regulations 2012

Requires colleges to publish certain information on its website:

[http://www.education.gov.uk/colleges/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestocollegeinformationregulations](http://www.education.gov.uk/schools/toolsandinitiatives/cuttingburdens/b0075738/reducing-bureaucracy/requirements/changestoschoolinformationregulations)

**Links to other organisations or documents**

The following links may help those who are developing or reviewing a college Online Safety policy.

**UK Safer Internet Centre**

[Safer Internet Centre -](http://www.saferinternet.org.uk/)

[South West Grid for Learning](http://www.swgfl.org.uk/Staying-Safe)

[Childnet](http://www.childnet-int.org/)

[Professionals Online Safety Helpline](http://www.saferinternet.org.uk/about/helpline)

[Internet Watch Foundation](https://www.iwf.org.uk/)

**CEOP**

<http://ceop.police.uk/> [ThinkUKnow](http://www.thinkuknow.co.uk/)

**Others:**

INSAFE - <http://www.saferinternet.org/ww/en/pub/insafe/index.htm>

UK Council for Child Internet Safety (UKCCIS) [www.education.gov.uk/ukccis](http://www.education.gov.uk/ukccis)

Netsmartz <http://www.netsmartz.org/index.aspx>

**Support for Colleges**

Specialist help and support  [SWGfL BOOST](http://www.swgfl.org.uk/boost)

**Cyberbullying**

Scottish Anti-Bullying Service, Respectme - <http://www.respectme.org.uk/>

Scottish Government [Better relationships, better learning, better behaviour](http://www.scotland.gov.uk/Publications/2013/03/7388)

[DCSF - Cyberbullying guidance](http://digizen.org/downloads/cyberbullyingOverview.pdf)

[DfE – Preventing & Tackling Bullying – Advice to college leaders, staff and Governing Bodies](http://webarchive.nationalarchives.gov.uk/20130401151715/https%3A/www.education.gov.uk/publications/standard/AllPublications/Page1/DFE-00062-2011)

Anti-Bullying Network - <http://www.antibullying.net/cyberbullying1.htm>

Cyberbullying.org - <http://www.cyberbullying.org/>

**Social Networking**

Digizen – [Social Networking](http://digizen.org/socialnetworking/)

[SWGfL - Facebook - Managing risk for staff and volunteers working with children and young people](http://360safe.org.uk/Files/Documents/facebook-6)

[Connectsafely Parents Guide to Facebook](http://www.connectsafely.org/Safety-Advice-Articles/facebook-for-parents.html)

[Facebook Guide for Educators](http://www.360safe.org.uk/Files/Documents/Facebook-Guide-for-Educators.aspx)

**Curriculum**

53

[SWGfL Digital Literacy & Citizenship curriculum](http://www.swgfl.org.uk/digitalliteracy)

Glow - <http://www.educationscotland.gov.uk/usingglowandict/>

Alberta, Canada - [digital citizenship policy development guide.pdf](http://education.alberta.ca/media/6735100/digital%20citizenship%20policy%20development%20guide.pdf)

Teach Today – [www.teachtoday.eu/](file:///F%3A%5CDropbox%5CE-S%20School%20Policy%20Docs%5Cwww.teachtoday.eu%5C)

Insafe - [Education Resources](http://lreforschools.eun.org/web/guest/insafe)

Somerset - [e-Sense materials for colleges](https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/e-safety%20pages/e-sense%20for%20schools.aspx)

**Mobile Devices / BYOD**

53

Cloudlearn Report [Effective practice for colleges moving to end locking and blocking](http://www.360safe.org.uk/Files/Documents/Cloudlearn_Report-end-to-locking-and-blocking.aspx)

NEN - [Guidance Note - BYOD](http://www.360safe.org.uk/Files/Documents/NEN_Guidance_Note_5_BYOD.aspx)

**Data Protection**

Information Commissioners Office:

[Your rights to your information – Resources for Colleges - ICO](http://www.ico.org.uk/schools)

[ICO pages for young people](http://www.ico.org.uk/youth)

[Guide to Data Protection Act - Information Commissioners Office](http://www.ico.gov.uk/for_organisations/data_protection_guide.aspx)

[Guide to the Freedom of Information Act - Information Commissioners Office](http://www.ico.gov.uk/for_organisations/freedom_of_information/guide.aspx)

[ICO guidance on the Freedom of Information Model Publication Scheme](http://www.ico.gov.uk/for_organisations/freedom_of_information/guide/publication_scheme.aspx)

[ICO Freedom of Information Model Publication Scheme Template for colleges](http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/schools_england_mps_final.pdf) (England)

[ICO - Guidance we gave to colleges - September 2012](http://www.360safe.org.uk/Files/Documents/ICO-guidance-for-schools-Sept-2012.aspx) (England)

[ICO Guidance on Bring Your Own Device](http://www.360safe.org.uk/Files/Documents/ico_bring_your_own_device_byod_guidance.aspx)

[ICO Guidance on Cloud Hosted Services](http://www.360safe.org.uk/Files/Documents/ICO-cloud_computing_guidance_for_organisations-1.aspx)

[Information Commissioners Office good practice note on taking photos in colleges](http://360safe.org.uk/Files/Documents/ICO-Good-Practice-Note-on-taking-photos-in-schools%22%20%5Ct%20%22_blank)

[ICO Guidance Data Protection Practical Guide to IT Security](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/it_security_practical_guide.ashx)

[ICO – Think Privacy Toolkit](http://www.ico.org.uk/for_organisations/training/think-privacy-toolkit)

[ICO – Personal Information Online – Code of Practice](http://www.ico.org.uk/for_organisations/guidance_index/~/media/documents/library/Data_Protection/Detailed_specialist_guides/personal_information_online_cop.ashx)

[ICO – Access Aware Toolkit](http://www.ico.org.uk/for_organisations/training/access-aware-toolkit)

[ICO Subject Access Code of Practice](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Detailed_specialist_guides/subject-access-code-of-practice.PDF)

[ICO – Guidance on Data Security Breach Management](http://www.ico.org.uk/for_organisations/data_protection/~/media/documents/library/Data_Protection/Practical_application/guidance_on_data_security_breach_management.pdf)

SWGfL - [Guidance for Colleges on Cloud Hosted Services](http://www.360safe.org.uk/Files/Documents/SWGfL-guidance-on-Cloud-hosting.aspx)

LGfL - [Data Handling Compliance Check List](http://files.lgfl.net/esafety/guides/check%20list%20for%20data%20handling%20best%20practice_jan2013.pdf)

Somerset - [Flowchart on Storage of Personal Data](https://slp.somerset.gov.uk/cypd/elim/somersetict/Site%20Pages/Data%20Protection.aspx)

NEN - [Guidance Note - Protecting College Data](http://www.360safe.org.uk/Files/Documents/NEN_Guidance_Note_1_protecting_school_data.aspx)

**Professional Standards / Staff Training**

DfE - [Safer Working Practice for Adults who Work with Children and Young People](http://360safe.org.uk/Files/Documents/Extracts-from-Guidance-for-Safer-Working-Practice-%22%20%5Ct%20%22_blank)

Kent - [Safer Practice with Technology](http://www.kenttrustweb.org.uk/UserFiles/CW/File/Advisory_Service_ICT/E-Safety/SaferPracticeWithTechnology-260509.pdf)

[Childnet / TDA - Social Networking - a guide for trainee teachers & NQTs](http://360safe.org.uk/Files/Documents/ChildnetSNSleaflet%283%29)

[Childnet / TDA - Teachers and Technology - a checklist for trainee teachers & NQTs](http://360safe.org.uk/Files/Documents/Childnettechnologyleaflet%284%29)

[UK Safer Internet Centre Professionals Online Safety Helpline](http://www.saferinternet.org.uk/helpline)

**Infrastructure / Technical Support**

Somerset - [Questions for Technical Support](http://www.360safe.org.uk/Files/Documents/Questions-for-Technical-Support-Somerset.aspx)

NEN -  [Guidance Note - esecurity](http://www.360safe.org.uk/Files/Documents/NEN_Guidance_Note_4_esecurity.aspx%22%20%5Ct%20%22_blank)

**Working with parents and carers**

SWGfL / Common Sense Media Digital Literacy & Citizenship Curriculum

 [SWGfL BOOST Presentations - parents presentation](http://www.swgfl.org.uk/boost)

[Connect Safely - a Parents Guide to Facebook](http://www.fbparents.org/)

[Vodafone Digital Parents Magazine](http://parents.vodafone.com/)

[Childnet Webpages for Parents & Carers](http://www.childnet.com/parents-and-carers)

[DirectGov - Internet Safety for parents](http://www.direct.gov.uk/en/Parents/Yourchildshealthandsafety/Internetsafety/index.htm)

[Get Safe Online - resources for parents](http://www.getsafeonline.org/nqcontent.cfm?a_id=1182)

[Teach Today - resources for parents workshops / education](http://www.teachtoday.eu/en/Lesson-Plans/Primary_Secondary/Parent_Workshop_Template_For_Schools.aspx)

[The Digital Universe of Your Children - animated videos for parents (Insafe)](http://www.saferinternet.org/digitaluniverse)

[Cerebra - Learning Disabilities, Autism and Internet Safety - a Parents' Guide](http://www.360safe.org.uk/Files/Documents/Learning-Disabilities%2C-Autism-and-Internet-Safety.aspx)

[Insafe - A guide for parents - education and the new media](http://www.360safe.org.uk/Files/Documents/e-safety_booklet-a-Guide-for-Parents-INSAFE.aspx)

[The Cybersmile Foundation (cyberbullying) - advice for parents](http://www.cybersmile.org/advice-help/category/advice-parents-1)

**Research**

[EU Kids on Line Report - "Risks and Safety on the Internet" - January 2011](http://360safe.org.uk/Files/Documents/EU-Kids-on-Line-Executive_Summary_Full_Findings-Ja)

[Futurelab - "Digital participation - its not chalk and talk any more!"](http://360safe.org.uk/Files/Documents/FutureLab-Digital-participation--its-not-chalk-and)

**Glossary of terms**

AUP Acceptable Use Policy – see templates earlier in this document

CEOP Child Exploitation and Online Protection Centre (part of UK Police, dedicated to protecting children from sexual abuse, providers of the Think U Know programmes.

CPC Child Protection Committee

CPD Continuous Professional Development

CYPS Children and Young Peoples Services (in Local Authorities)

FOSI Family Online Safety Institute

EA Education Authority

ES Education Scotland

HWB Health and Wellbeing

ICO Information Commissioners Office

ICT Information and Communications Technology

ICTMark Quality standard for colleges provided by NAACE

INSET In Service Education and Training

IP address The label that identifies each computer to other computers using the IP (internet protocol)

ISP Internet Service Provider

ISPA Internet Service Providers’ Association

IWF Internet Watch Foundation

LA Local Authority

LAN Local Area Network

MIS Management Information System

NEN National Education Network – works with the Regional Broadband Consortia (e.g. SWGfL) to provide the safe broadband provision to colleges across Britain.

55

Ofcom Office of Communications (Independent communications sector regulator)

SWGfL South West Grid for Learning Trust – the Regional Broadband Consortium of SW Local Authorities – is the provider of broadband and other services for colleges and other organisations in the SW

TUK Think U Know – educational Online Safety programmes for colleges, young people and parents.

VLE Virtual Learning Environment (a software system designed to support teaching and learning in an educational setting,

WAP Wireless Application Protocol

56

54

57