

**On-line Safety Policy**

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

4

This On-line Safety policy has been developed in collaboration with.

DSL for Child Protection/Safeguarding

Members of SLT

On-Line Safety Coordinator

Staff – including teachers, support staff, technical staff

Governors

Parents, carers and students

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

**Schedule for Development / Monitoring / Review**

5

|  |  |
| --- | --- |
| This On-line Safety policy was approved by the *Governing Body* |  |
| The implementation of this On-line 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 On-line Safety policy generated by the monitoring group (which will include anonymous details of On-line Safety incidents) at regular intervals: | *At least once a year* |
| The On-line 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 On-line Safety or incidents that have taken place. |  |
| Should serious On-line Safety incidents take place, the following external persons / agencies should be informed: | *LA ICT Manager, 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

• 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 On-line 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 On-line Safety behaviour that take place out of college.

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

This On-line 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 On-line Safety roles and responsibilities of individuals and groups within the college.

**Governors:**

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

*•* regular meetings with the On-line Safety Co-ordinator

• regular monitoring of On-line 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 On-line Safety) of members of the college community, though the day to day responsibility for On-line Safety will be delegated to the On-line 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 On-line Safety allegation being made against a member of staff**.** (see flow chart on dealing with On-line Safety incidents).

*•* 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 On-line 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 On-line 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 On-line Safety Co-ordinator *.*

**On-line Safety Coordinator: (DSL Child Protection/Safeguarding)**

• leads the On-line Safety committee

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

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

• provides training and advice for staff

• liaises with the Local Authority

• liaises with college technical staff

• receives reports of On-line Safety incidents and creates a log of incidents to inform future On-line Safety developments

• meets regularly with On-line 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 the facilities management provider 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 On-line 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 (see appendix “Technical Security Policy ” for good practice).

• that the use of the network / internet / remote access attempted misuse can be reported to the Headteacher / Senior Leader; On-line 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 On-line Safety matters and of the current college On-line 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 Headteache, SLT or On-line 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 .

• On-line Safety issues are embedded in all aspects of the curriculum and other activities .

• students understand and follow the On-line 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 should be trained in On-line 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 on-line contact with adults / strangers

• potential or actual incidents of grooming

• cyber-bullying

**On-line Safety Group**

The On-line Safety Group provides a consultative group that has wide representation from the college community, with responsibility for issues regarding On-line Safety and the monitoring the On-line 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 On-line Safety Group (or other relevant group) will assist the On-line Safety Coordinator with:

• the production / review / monitoring of the college On-line Safety policy / documents.

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

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

*•* monitoring network / internet / incident logs.

*•* consulting stakeholders – including parents / carers and the students about the On-line 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 On-line Safety practice when using digital technologies out of college and realise that the college’s On-line 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, website / VLE and information about national / local On-line Safety campaigns / literature*.* Parents and carers will be encouraged to support the college in promoting good On-line 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 on-line 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 On-line Safety is therefore an essential part of the college’s On-line Safety provision. Children and young people need the help and support of the college to recognise and avoid On-line Safety risks and build their resilience.

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

* A planned On-line Safety curriculum provided as part of Computing and ID lessons and regularly revisited
* Key On-line 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 on-line 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 On-line Safety practice when using digital technologies out of school and realise that the college’s On-line 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 On-line 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 on-line 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 On-line Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

• A planned programme of formal On-line Safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the On-line Safety training needs of all staff will be carried out regularly.

• All new staff should receive On-line Safety training as part of their induction programme, ensuring that they fully understand the college On-line 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 On-line Safety policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days.

• The On-line Safety Coordinator will provide advice / guidance / training to individuals as required.

Training – Governors

Governors should take part in On-line Safety training / awareness sessions, with particular importance for those who are members of any sub-committee / group involved in technology / On-line 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 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 CEO 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. Monitoring is carried out.

• An appropriate system is in place for users to report any actual / potential technical incident / security breach to the On-line Safety co-ordinator.

• Appropriate security measures are in place through the facilities management provider 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. These are tested regularly. 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 are welcome to take videos and digital images of their children at college events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone’s privacy and in some cases protection, these images should not be published / made publicly available on social networking sites, nor should parents / carers comment on any activities involving other students in the digital / video images.

• 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.

• Students’ full names will not be used anywhere on a website or blog, particularly in association with photographs.

• 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.

• 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 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”**. (**see Privacy Notice section in the appendix)
* It complies with a Data Protection Policy
* It is registered as a Data Controller for the purposes of the Data Protection Act (DPA)
* Risk assessments are carried out
* 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 full on-line safety policy can be viewed on request.**