Online Safety Policy

Unity College

ADOPTED September 2023

NEXT REVIEW September 2024

Contents

Aims

Unity College aims to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers and governors
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole college community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The four key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as child-on-child pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-**nudes** and/or pornography), sharing other explicit images and online bullying; and
- Commerce – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

Legislation and Guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, **Keeping Children Safe in Education**, and its advice for schools on:

- **Teaching online safety in schools**
- **Preventing and tackling bullying** and **cyber-bullying: advice for headteachers and school staff**
- **Relationships and sex education**
- **Searching, screening and confiscation**

It also refers to the DfE's guidance on **protecting children from radicalisation**.

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

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

Roles and Responsibilities

3.1 The governing body

The governing body has overall responsibility for monitoring this policy and holding the Headteacher to account for its implementation.

The governing board will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The governing board will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The governing board will co-ordinate regular meetings with appropriate staff to discuss online safety, requirements for training, and monitor online safety logs as provided by the designated safeguarding lead (DSL).

The governing board should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governing board must ensure the school has appropriate filtering and monitoring systems in place on college devices and college networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and service providers what needs to be done to support the school in meeting those standards, which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems
- Reviewing filtering and monitoring provisions at least annually
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning
- Having effective monitoring strategies in place that meet their safeguarding needs

The governor who oversees online safety is Richard Kelly.

All governors will:

- Ensure that they have read and understand this Policy
- Agree and adhere to the terms on acceptable use of the College's ICT systems and the internet (*Appendix* 2)
- Ensure that online safety is a running and interrelated theme while devising and implementing their whole college approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some students with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.2 The Headteacher

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

3.3 The Designated Safeguarding Lead

Details of the College's designated safeguarding lead (DSL) are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions.

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

- Supporting the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the Headteacher, Deputy Headteacher and governing board to review this Policy annually and ensure the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on college devices and school networks
- Working with the Network Manager to make sure the appropriate systems and processes are in place

- Working with the Headteacher, Network Manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the College's Child Protection and Safeguarding Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this Policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the College's Behaviour Policy
- Updating and delivering staff training on online safety (*Appendix 3* contains a self-audit for staff on online safety training needs)
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in college to the Headteacher and/or governing board
- Undertaking annual risk assessments that consider and reflect the risks children face
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.4 The Director of Resources

The Director of Resources is responsible for:

- Ensuring that Unity College uses Lancashire County Council's ICT infrastructure system to monitor all ICT systems which provides updates and reports, as required any security breaches including, and not limited to, specific reports on student or staff misuse
- Ensuring that any online security breaches identified are reported to the appropriate person

This list is not intended to be exhaustive.

3.5 The Network Manager

The Network Manager is responsible for:

- Putting in place an appropriate level of security protection procedures, such as filtering and monitoring systems on college devices and college networks, which are reviewed and updated at least annually to assess effectiveness and ensure pupils are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the College's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Conducting a full security check and monitoring the College's ICT systems on a weekly basis
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this Policy

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this Policy
- Implementing this Policy consistently

- Agreeing and adhering to the terms on acceptable use of the College's ICT systems and the internet (*Appendix* 2), and ensuring that students follow the College's terms on acceptable use (*Appendices 1 and 1*)
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the College's Behaviour Policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.7 Parents and carers

Parents and carers are expected to:

- Notify a member of staff or the Headteacher of any concerns or queries regarding this Policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the College's ICT systems and internet (*Appendix 1*)
- Parents and carers can seek further guidance on keeping children safe online from the following organisations and websites:
    - What are the issues? **UK Safer Internet Centre**
    - Hot topics **Childnet International**
    - Parent/carer resource sheet **Childnet International**

3.8 Visitors and members of the community

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

Educating Students about Online Safety

Students will be taught about online safety as part of the curriculum. **All** schools have to teach **Relationships and sex education and health education**.

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

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

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

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

By the **end of secondary school**, students will know:

- Their rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online
- About online risks, including that any material someone provides to another has the potential to be shared online and the difficulty of removing potentially compromising material placed online

- Not to provide material to others that they would not want shared further and not to share personal material which is sent to them
- What to do and where to get support to report material or manage issues online
- The impact of viewing harmful content
- That specifically sexually explicit material (*e.g. pornography*) presents a distorted picture of sexual behaviours, can damage the way people see themselves in relation to others and negatively affect how they behave towards sexual partners
- That sharing and viewing indecent images of children (including those created by children) is a criminal offence which carries severe penalties including jail
- How information and data is generated, collected, shared and used online
- How to identify harmful behaviours online (including bullying, abuse or harassment) and how to report, or find support, if they have been affected by those behaviours
- How people can actively communicate and recognise consent from others, including sexual consent, and how and when consent can be withdrawn (in all contexts, including online)

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

Where necessary, teaching about safeguarding, including online safety, will be adapted for vulnerable children, victims of abuse, EAL students and some students with SEND.

Educating Parents and Carers about Online Safety

The College will raise parents' and carers' awareness of internet safety in letters or other communications home, and in information via our website or via our online communication portal. This Policy will also be shared with parent and carers.

Online safety will also be covered during parents' evenings.

The College will let parent and carers know:

- What systems the College uses to filter and monitor online use
- What their children are being asked to do online, including the sites they will be asked to access and who from the College (if anyone) their child will be interacting with online
- If parent and carers have any queries or concerns in relation to online safety, these should be raised in the first instance with the Headteacher and/or the DSL

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

Cyber-Bullying

6.1 Definitions

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

6.2 Preventing and addressing cyber-bullying

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

The College will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. PD tutors and subject teachers will discuss cyber-bullying with their groups.

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

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

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

In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College's Behaviour Policy and Anti-Bullying Policy. Where illegal, inappropriate or harmful material has been spread among students, the College will use all reasonable endeavours to ensure the incident is contained.

The DSL will report the incident and provide the relevant material to the police as soon as is reasonably practicable, if they have reasonable grounds to suspect that possessing that material is illegal. They will also work with external services if it is deemed necessary to do so.

6.3 Examining electronic devices

The Headteacher, and any member of staff authorised to do so by the Headteacher (as set out in the College's Behaviour Policy and Searching, Screening and Confiscation Policy), can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:

- Poses a risk to staff or students, *and/or*
- Is identified in the College rules as a banned item for which a search can be carried out, *and/or*
- Is evidence in relation to an offence

Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:

- Make an assessment of how urgent the search is, and consider the risk to other students and staff. If the search is not urgent, they will seek advice from the DSL
- Explain to the student why they are being searched, how the search will happen, and give them the opportunity to ask questions about it
- Seek the student's cooperation

Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.

When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:

- Cause harm, *and/or*
- Undermine the safe environment of the college or disrupt teaching, *and/or*
- Commit an offence

If inappropriate material is found on the device, it is up to the DSL to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.

When deciding if there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:

- They reasonably suspect that its continued existence is likely to cause harm to any person, *and/or*
- The student and/or the parent or carer refuses to delete the material themselves

If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:

- **Not** view the image
- Confiscate the device and report the incident to the DSL immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on **screening, searching and confiscation** and the UK Council for Internet Safety (UKCIS) guidance on **sharing nudes and semi-nudes: advice for education settings working with children and young people**

Any searching of students will be carried out in line with:

- The DfE's latest guidance on **searching, screening and confiscation**
- UKCIS guidance on **sharing nudes and semi-nudes: advice for education settings working with children and young people**
- Our Searching, Screening and Confiscation Policy
- Our Behaviour Policy

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the College's Complaints Procedure.

6.4 Artificial intelligence (AI)

Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents and carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

Unity College recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real.

Unity College will treat any use of AI to bully students in line with our Behaviour Policy and Anti-Bullying Policy.

Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the College.

Acceptable Use of the Internet in College

All students, parents and carers, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of the College's ICT systems and the internet (*Appendices 1 and 2*). Visitors will be expected to read and agree to the College's terms on acceptable use if relevant.

Use of the College's internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by students, staff, volunteers, governors and visitors (where relevant) to ensure they comply with the above.

Students Using Mobile Devices in College

Student are prohibited from using mobile phones anywhere on the College grounds. Sanctions for breaching the policy are detailed in the Behaviour Policy.

Any use of other mobile devices, such as laptops, in college by students must be in line with the acceptable use agreement (see *Appendix 1*).

Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the College's Behaviour Policy, which may result in the confiscation of their device.

Staff Using Work Devices Outside College

All staff members will take appropriate steps to ensure their devices remain secure. This includes, but is not limited to:

- Keeping the device password-protected. Strong passwords are at least 8 characters, with a combination of upper and lower-case letters, numbers and special characters (e.g. asterisk or currency symbol)
- Making sure the device locks if left inactive for a period of time
- Not sharing the device among family or friends
- Keep pre-installed anti-virus and anti-spyware software
- Keeping operating systems up to date by always installing the latest updates

Staff members must not use the device in any way which would violate the College's terms of acceptable use, as set out in *Appendix 2*.

If staff have any concerns over the security of their device, they must seek advice from the Network Manager.

How the College Will Respond to Issues of Misuse

Where a student misuses the College's ICT systems or internet, we will follow the procedures set out in our Behaviour Policy and Acceptable Use Agreement. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the College's ICT systems or the internet, or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the Staff Disciplinary Procedures and Staff Code of Conduct. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.

The College will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

Training

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

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

By way of this training, all staff will be made aware that:

- Technology is a significant component in many safeguarding and wellbeing issues, and that children are at risk of online abuse
- Children can abuse their peers online through:
    - Abusive, harassing, and misogynistic messages

    - Non-consensual sharing of indecent nude and semi-nude images and/or videos, especially around chat groups
    - Sharing of abusive images and pornography, to those who don't want to receive such content
- Physical abuse, sexual violence and initiation/hazing type violence can all contain an online element

Training will also help staff:

- Develop better awareness to assist in spotting the signs and symptoms of online abuse
- Develop the ability to ensure students can recognise dangers and risks in online activity and can weigh up the risks
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

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

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

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Child Protection and Safeguarding Policy.

Monitoring Arrangements

This Policy will be reviewed **annually** by the Deputy Headteacher (Alison Hodgson) and Lead DSL (Bev Worthington). At every review, the Policy will be shared with the governing body's Community Partnerships Committee.

The review will be supported by an annual risk assessment that considers and reflects the risks students face online. This is important because technology, and the risks and harms related to it, evolve and change rapidly.

Links with Other Policies

This Online Safety Policy is linked to our:

- Child Protection and Safeguarding Policy
- Behaviour Policy
- Searching, Screening and Confiscation Policy
- Staff disciplinary procedures
- Data Protection Policy and privacy notices
- Complaints Procedure
- ICT and internet acceptable use policies

Appendix 1 ICT Acceptable Use Policy (Students)

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

This Student Acceptable Use Policy is intended to ensure:

- That young people will be responsible users and stay safe whilst using the internet and other digital technologies for educational, personal and recreational use
- That Unity College systems and users are protected from accidental or deliberate misuse that could put the security of the systems and/or 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

This Student Acceptable Use Policy relates to:

- The use of college systems and devices (both inside and outside of Unity College)
- The use of own devices within college (where allowed) e.g. mobiles phones, cameras etc.
- The use of own equipment out of the College in a way that is related to being a member of Unity College e.g. communicating with other members of the college, accessing college email, VLE, website etc.

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

Acceptable Use Policy Agreement Statement:

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

I agree the following:

1. For my own personal safety:

- I understand that the College will monitor my use of the systems, devices and my 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 and financial details, amongst others)
- If I arrange to meet people offline 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 materials, messages or anything that makes me feel uncomfortable when I see it online

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

- 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 may take up internet capacity and prevent other users from being able to carry out their work
- I will not use the College system or devices for online gambling, internet shopping, file sharing or video broadcasting, unless I have permission from a member of staff to do so
- I will only print college work with staff permission and I will not intentionally waste limited resources such as paper or printer ink
- At the end of each session, I will close all programmes and log out of the device and college systems

3. I will act as a 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, therefore 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

4. I recognise that Unity College has a responsibility to maintain the security and integrity of the technology it offers and to ensure the smooth running of systems within college:

- I will only use my personal devices in college if I have permission. I understand that, if I do use my own device within 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 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 or attachments in emails, unless I know and trust the person or 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 a college device, nor will I try to alter computer settings
- I will not use mobile devices to take pictures / videos in college unless given permission to do so by a member of staff
- I will not use social media during the College day

5. 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

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

- I understand that the College 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 *(e.g. cyber-bullying, use of images, sharing of personal information etc.)*

- 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 Unity College network / internet, consequences outlined in the Behaviour Policy and in the event of illegal activities, involvement of the police

Appendix 2 ICT Acceptable Use Policy (Staff, Governors, Volunteers and Visitors)

New technologies have become integral to the lives of children and young people in today's society, both within college 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 raise 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 Staff Acceptable Use Policy is intended to ensure:

- That staff, governors, volunteers and visitors 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, governors, volunteers and visitors are protected from potential risk in their use of ICT in their everyday work.
- That staff, governors, volunteers and visitors comply with college policies on Data Protection, Safeguarding and Child Protection, Online Safety and the Staff Code of Conduct.

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 and will, in return, expect staff, governors, volunteers and visitors 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 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 College will 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 all college ICT systems 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.
- 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.
- I will abide by the College Online Safety Policy.

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 only do so with their permission and in accordance with the College's Data Protection Policy and Photography and Video Consent Use and Storage Policy.
- I will not use photographs/video of students if permission has not been granted by parents or carers.
- I will not write, send, publish, copy, distribute or forward derogatory or defamatory remarks about any person or organisation, either on the internet or by email. If I discover potentially defamatory material, I will report it to a member of the Senior Leadership Team (SLT) immediately.
- I will not use chat or social networking sites in college for any reason. I will ensure that social networking site notifications are not delivered whilst in college.
- I will ensure that my personal social networking sites are set to private; that students are never listed as approved contacts and consider carefully any friend requests. I will never use or access social networking sites of students.
- I will only communicate with students and parents/carers using official college systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I will never give my personal contact details to students, including social networking, email and mobile communications/messaging services.

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) 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.
- USB devices are not to be used in college without the permission of college management.
- 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 understand that data is automatically backed up for me if it is stored on the network or on OneDrive, but not if it is stored locally. I understand that I have a duty to make sure that work related data and student data is backed up and secure.
- 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 only print essential resource material and will always check that the length of a document is reasonable before printing.
- 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, without the express permission of college management.

- I will not disable or cause any damage to college equipment, or the equipment belonging to others. I will not unplug any wires connected to desktops or projectors without the permission of college management.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the College's Data Protection Policies. 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 therefore not give out personal addresses, telephone number or email addresses of any staff or students at the College, unless formally requested to do so by the Headteacher.
- 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 and / or the Local Authority and in the event of illegal activities the involvement of the police.

I will ensure that I keep up-to-date with any changes to this policy.

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 / Visitor Name

Signed

Date

Appendix 3 Online Safety Training Needs Staff Self-Audit

ONLINE SAFETY TRAINING NEEDS AUDIT	
Name	**Date**
Question	**Yes/No (add comments if necessary)**
Do you know the name of the person who has lead responsibility for online safety in college?	
Are you aware of the ways in which students can abuse their peers online?	
Do you know what you must do if a student approaches you with a concern or issue?	
Are you familiar with the College's Acceptable Use Agreement for staff, volunteers, governors and visitors?	
Are you familiar with the College's Acceptable Use Agreement for students?	
Do you regularly change your password for accessing the College's ICT systems?	
Are you familiar with the College's approach to tackling cyber-bullying?	
Are there any areas of online safety in which you would like further training?	