Online Safety Policy

2023 - 2024

Scope of the Policy

This policy applies to all member of the College community (including visitors) who have access to and are users of our College digital technology systems, both in and out of the College. The Online Safety policy should be read alongside the Safeguarding Policy, Behaviour Policy and Anti-Bullying Policy and Staff Code of Conduct.

Online safety is part of a school/college's statutory safeguarding responsibilities. Keeping Children Safe in Education (2022) makes clear the specific responsibilities around Online Safety. It says:

"It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate students, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate."

KCSIE (2022) outlines four areas of risk:

- Content: Being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation and extremism.
- Contact: Being subjected to harmful online interaction with other users; for example: 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; for example, 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

This policy is based on the Department for Education's (DfE) 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.

The College will 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.

Roles and Responsibilities

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 and compliance with Keeping Children Safe in Education (2022). 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 as part of their role as Safeguarding Governor. The role will include:

- Meetings with the Online Safety Lead
- Reviewing online safety incident logs, filtering and monitoring systems, development plans

- Reporting to relevant Governor Board meetings

Headteacher / 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 Lead.
- 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 (see flow chart on dealing with online safety incidents "Responding to incidents of misuse" and relevant Local Authority disciplinary procedures).
- The Headteacher will ensure that the Online Safety Lead and 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 will ensure that the Online Safety Lead is given support by the Designated Safeguarding Lead (DSL). This is to provide a clear link to the wider safeguarding work of the College and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive termly monitoring reports from the Online Safety Lead.

Designated Safeguarding Lead

Details of the College's DSL and deputies are set out in our Child Protection and Safeguarding Policy as well as relevant job descriptions. The DSL should:

- Support the Headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the College
- Working with the Headteacher, Online Safety Lead and other staff, as necessary, to address any online safety issues or incidents
- Ensure the Online Safety Lead is implementing the policy in line with the current Keeping Children Safe in Education and other best practice
- Ensure that Online Safety is part of the annual staff CPD calendar and new staff induction
- Support the Heads of Subject in updating relevant areas of the College curriculum annually

Online Safety Lead

- Takes day to day responsibility for online safety issues, supported by the College SLT
- Has a leading role in establishing and reviewing the College online safety policies / documents and planning for improving College practice
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place, in line with Keeping Children Safe in Education and the College Safeguarding Policy
- Provides up to date training and advice for staff, for example on harmful online challenges and online hoaxes
- Liaises with the Local Authority
- Liaises with College technical staff
- Reports regularly on the Online Safety Development Plan to Senior Leadership Team and Governors
- Meets regularly with the DSL to inform the Online Safety Development Plan
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Liaises with SLT following Online Safety incidents to inform their decisions about any consequences
- Will set up and lead and Online Safety working group, made up of a range of staff

Network Manager / Technical staff

The College currently contracts management of the network to an external contractor. As part of our Service Level Agreement, they ensure:

- That the College's technical infrastructure is secure and is not open to misuse or malicious attack
- That the College meets required online safety technical requirements,
- That users may only access the networks and digital devices through a properly enforced password protection policy, in which passwords are regularly changed

- The filtering policy is applied and updated on a regular basis and that its implementation is not the sole responsibility of any single person
- That they keep up to date with online safety technical information in order to effectively carry out their online safety role and to inform and update others as relevant
- That the use of the network / internet / Learning Platform / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Online Safety Lead or SLT for investigation / action / sanction
- That monitoring software / systems are implemented and updated as agreed in College policies

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 Online Safety Lead or SLT for investigation / action / sanction, including during any online learning activities and remote learning
- All digital communications with students / parents / carers should be on a professional level and only carried out using official College systems
- Online safety issues, including the 4 Cs, are embedded in all aspects of the curriculum and other activities
- Students understand and follow the Online Safety Policy 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 digital devices, cameras etc. in lessons and other College activities (where allowed) and implement current policies with regard to these digital 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
- Will ensure that any portable digital devices used to store data is securely encrypted, and any loss of data is immediately reported to the Online Safety Lead.

Students / Students:

- Are responsible for using the College digital technology systems in accordance with the Student Acceptable Use Agreement, including during any online learning activities
- 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 digital devices and digital cameras. They should also know and understand policies on the taking / use of images and on online-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 digital devices in an appropriate way. The College will take every opportunity to help parents understand these issues through Parents' Evenings, newsletters, letters, website / app 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:

- Online learning platforms and resources
- Digital and video images taken at College events
- Access to parents' sections of the website / learning platform and online student / student records
- Their children's personal digital devices in the College

Parents 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 resource sheet Childnet International
- Healthy relationships Disrespect Nobody

Community Users

Community Users who access the College's IT provision will be expected to sign a Community User AUA before being provided with access to any College system. (A Community Users Acceptable Use Agreement Template can be found in the appendices.)

Education (Students)

Students will be taught about online safety as part of the curriculum which incorporates the DfE guidance on relationships education, relationships and sex education (RSE) and health education. This states that schools have to teach:

- Relationships and sex education and health education in secondary schools
- 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 their time at Denton Community College 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)

Online safety should be a focus in all areas of the curriculum and staff should reinforce online safety messages across the curriculum. Staff should act as good role models in their use of digital technologies, the internet and mobile digital devices. 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 and some students with SEND.

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 / digital literacy 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.

- In lessons where internet use is pre-planned, it is best practice that 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.
- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination) that would normally result in internet searches being blocked. In such a situation, staff can request that the Technical Staff (or other relevant designated person) can temporarily remove those sites 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:

- Letters, newsletters, web site, app
- Parents / Carers evenings / sessions
- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications e.g. ThinkUKnow and NetAware

Education (The Wider Community)

The College aims to provide opportunities for local community groups / members of the community to gain from the College's online safety knowledge and experience. This may be offered through the following:

- Providing family learning courses in use of new digital technologies, digital literacy and online safety
- Online safety messages targeted towards grandparents and other relatives as well as parents.
- The College website will provide online safety information for the wider community
- Developing Digital Leaders to support partner primary schools
- Supporting community groups e.g. Early Years Settings, Childminders, youth / sports / voluntary groups to enhance their Online Safety provision

Education & Training (Staff / Volunteers)

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

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- 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. This will be annually updated to include any new issues raised in Keeping Children Safe in Education.
- It is expected that some staff will identify online safety as a training need within the performance management process.
- The Online Safety Lead (or other nominated person) 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 presented to and discussed by staff.
- The Online Safety Lead (or other nominated person) will provide advice / guidance / training to individuals as required.

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 other children 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 the risks up
- Develop the ability to influence students to make the healthiest long-term choices and keep them safe from harm in the short term

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 /safeguarding. This may be offered in a number of ways:

- Attendance at training provided by the Local Authority / National Governors Association / or other relevant organisation (e.g. SWGfL).
- Participation in College training / information sessions for staff or parents (this may include attendance at assemblies / lessons).
- Training delivered as part of a Governors Meeting

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 which will explain the reasons why it occurs, the forms it may take and what the consequences can be.
- Form tutors will discuss cyber-bullying with their tutor groups.
- 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.
- The College also sends information/leaflets on cyber-bullying to parents so that they are aware of the signs, how to report it and how they can support children who may be affected.
- In relation to a specific incident of cyber-bullying, the College will follow the processes set out in the College Behaviour 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 consider whether the incident should be reported to the police if it involves illegal material, and will work with external services if it is deemed necessary to do so.

Mobile Technologies (including BYOD)

Mobile technology digital devices may be College owned/provided or personally owned and might include: smartphone, portable games console, tablet, notebook / laptop or other technology that usually has the capability of utilising the College's wireless network. The device then has access to the wider internet which may include the College's learning platform and other cloud based services such as email and data storage.

All users should understand that the primary purpose of the use mobile / personal digital devices in a College context is educational. Teaching about the safe and appropriate use of mobile technologies is an integral part of the College's Online Safety education programme.

Students may bring mobile devices into College, but are not permitted to use them during:

- Lessons / form time (unless it is for a teacher-directed activity)
- Movement around the building

Any use of mobile devices in College by students must be in line with the acceptable use agreement. Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the College Behaviour Policy, which may result in the confiscation of their device.

- The College BYOD network is secure, filtered and monitored when available to students in College.
- The password is regularly changed.
- The College Behavior Policy covers use of mobile digital devices outside of lesson times
- Education about the safe and responsible use of mobile digital devices is included in the College Online Safety curriculum

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 cyberbullying 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 e.g. on social networking sites.
- Written permission from parents or carers is obtained before photographs of students are published on the College website / social media / local press
- 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.
- Students must not take, use, share, publish or distribute images of others without their permission
- Students' full names will not be used online, particularly in association with photographs.

Examining Electronic Devices

College staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

If staff feel there is a 'good reason' to examine a device they must follow the College Behaviour Policy and / or Safeguarding Policy and alert the DSL / child protection team as they would any other behaviour or safeguarding incident in College.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt teaching, and/or
- Break any of the College rules

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of College discipline), and/or
- Report it to the police*

* Staff may also confiscate devices for evidence to hand to the police, if a student discloses that they are being abused and that this abuse includes an online element.

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

- The DfE's latest guidance on screening, searching and confiscation
- UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- The College's COVID-19 risk assessment

Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the College complaints procedure which can be found on the Denton Community College website..

Data Protection

Please see our Data Protection Policy for further information. It has been reviewed in line with the 2018 GDPR legislation.

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 digital devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected digital devices.

When personal data is stored on any portable computer system, memory stick or any other removable media:

- The data must be encrypted and password protected.
- The device must offer virus and malware checking software.
- The data must be securely deleted from the device, in line with College policy (below) once it has been transferred or its use is complete.

Communications

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

When using communication technologies, the College considers the following as good practice:

- The official College 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 Online Safety Lead or SLT 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, social media, chat, blogs, VLE etc.) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.

- Students should be taught about online safety issues, such as the risks attached to the sharing of personal details. They should also be taught strategies to deal with inappropriate communications and be reminded of the need to communicate appropriately when using digital technologies.

Technical (Infrastructure, Equipment, Filtering & Monitoring)

The College currently contracts management of the network to an external contractor. As part of our Service Level Agreement, and in partnership with LA technical support services, they ensure 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.

- 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
- All users will have clearly defined access rights to College technical systems and digital devices.
- All users will be provided with a username and secure password
- Users are responsible for the security of their username and password and will be required to change their password regularly
- The "master / administrator" passwords for the College ICT systems, used by the Network Manager (or other person) must also be available to the Headteacher and Finance Officer.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation CAIC list. 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 / monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet.
- Any security breach, including data loss, is reported immediately to the Online Safety Lead and SLT in College.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile digital 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.
- Personal data cannot be sent over the internet or taken off the College site unless safely encrypted or otherwise secured.
- All College laptops and other hardware are encrypted before being given out to staff.

Review of the Policy

This Online Safety Policy will be reviewed annually in consultation with:

- Headteacher
- Senior Leaders
- Online Safety Lead
- Staff (including Teachers, Support Staff & Technical Staff)
- Students

Other Linked Policies

The Online Safety policy should be read alongside the:

- Safeguarding Policy
- Behaviour Policy
- Anti-Bullying Policy
- Staff Code of Conduct.

Denton Community College

Staff Acceptable Use Agreement

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 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 technology in their everyday work.

Introduction:

I understand that I must use College systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology 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 College digital technology & communications systems. • I understand that the rules set out in this agreement also apply to use of technologies (e.g. laptops, email, social media etc.) out of College, and to the transfer of personal data (digital or paper based) out of College. • I understand that the College digital technology 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 code of conduct. • 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 only write down/store a password securely. • I will immediately report any illegal, inappropriate or harmful material or incident I become aware of.
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 it will not be possible to identify by name, or other personal information, those who are featured. • I will only use social networking sites in College in accordance with the staff code of conduct. • 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 on-line activity that may compromise my professional responsibilities or the reputation of the College. 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 will not share confidential information about the College, its students or staff, or other members of the community
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 digital devices (laptops / tablets / mobile phones / USB digital 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, including encryption and passwords. Will ensure that any such digital 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
- 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/attempt to install programmes or store programmes on a computer.
- 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 Data Protection 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 / 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, or any other issues involving my use of ICT, however this may have happened.

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

- I understand that this agreement applies not only to my work and use of College digital technology equipment in College, but also applies to my use of College 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.

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

Staff / Volunteer Name: ..... Signed: .....

Date: .....

Denton Community College

Student Acceptable Use Agreement

Denton Community College students will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use. Access to College systems and digital devices comes with agreeing to this document. You must stick to this agreement and follow these guidelines when:

- You use the College systems and digital devices both in and out of College
- You use your own digital devices in the College (when allowed) e.g. mobile phones, tablets, cameras etc.
- You use your own equipment out of the College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College email, social media, etc.

For my own personal safety:
• I understand that the College will monitor my use of the systems, digital 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 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, etc.) • I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online to parents/carers, College staff or via the CEOP website.
I will act as I expect others to act toward me:
• 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 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. • If I have concerns about another student's use of ICT (e.g. unsafe or risky behaviour; malicious or inappropriate behaviour online) I will report this to a member of staff to ensure that students at Denton, and our ICT systems, remain safe.
I understand that everyone has equal rights to use technology as a resource and:
• I understand that the College systems and digital 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 digital devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so. • I understand that any misuse of ICT will be followed up in line with the College Behaviour Policy
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 digital devices (mobile phones / USB / digital devices etc.) in College if I have permission. • I understand that, if I do use my own digital devices in the College, I will follow the rules set out in this agreement, in the same way as if I was using College equipment and that my behaviour is still covered by the College Behaviour Policy.

- 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
- 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 allowed.

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 College also 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, detentions, suspensions, contact with parents and in the event of illegal activities involvement of the police.
- If College has reason to believe any device has been used in illegal or other serious incidents, the device will be confiscated and kept securely while the incident is investigated.

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

- I use the College systems and digital devices both in and out of College
- I use my own digital devices in the College (when allowed) e.g. mobile phones, tablets, cameras etc.
- I use my own equipment out of the College in a way that is related to me being a member of this College e.g. communicating with other members of the College, accessing College email, social media, etc.