



Online Safeguarding Policy (including social media and UTC technical security policy)

Status:	Statutory
Member of Staff Responsible:	Designated Safeguarding Lead
Designated Person responsible for Safeguarding:	Assistant Principal / Principal (Designated Safeguarding Lead and Pastoral)
Deputy Designated Person responsible for Safeguarding:	Learning Managers
Governor with responsibility for Safeguarding:	Neil Bizzell

Associated policies and documentation:

- Behaviour Management
- Anti-bullying
- Health and Safety
- Financial Probity & Whistle Blowing
- Online Safety Policy
- Single Central Record
- Whistleblowing
- Staff Code of Conduct
- SCSB Reasonable Force Guidance

Implementation Date: September 2022

Reviewed Date: February 2026

Next Review Date: February 2027

Contents

Contents

Rationale	3
Development/Monitoring/Review of this Policy	4
Roles and Responsibilities	5
Policy Statements	7
Dealing with unsuitable/inappropriate activities	15
Responding to incidents of misuse.....	17
Illegal Incidents	18
Other Incidents.....	19
UTC actions & sanctions	19
UTC Technical Security Policy (including filtering and passwords)	23
Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.	28

Rationale

The requirement to ensure that children and young people can use the internet and related communications technologies appropriately and safely is addressed as part of the wider duty of care to which all who work in the UTC are bound. Our online safeguarding policy should help to ensure safe and appropriate use by all users and should ensure that personal data is protected.

The use of digital technologies in educational settings and at home is part of daily life and can bring great benefits and opportunities. However, there are also risks and it is important that these are understood and managed effectively so a good balance is achieved. It is essential that the online safeguarding policy is used in conjunction with and referenced in the Child Protection/Safeguarding policy and other policies such as Anti-bullying, Behaviour, Code of Conduct etc. The breadth of issues within online safeguarding is considerable, but they can be categorised into three areas of risk:-

Content: being exposed to illegal, inappropriate or harmful material

Contact: being subjected to harmful online interaction with other users including sexual exploitation, radicalisation and extremism

Conduct: personal online behaviour that increases the likelihood of, or causes, harm.

Scope of the Policy

This policy applies to all members of the UTC community (including staff, Board of Trustees / Governors, students / students, volunteers, parents / carers, work placement students, visitors, community users) who have access to and are users of our ICT systems, both in and out of the UTC building.

- **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 UTC site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other Online Safeguarding incidents covered by this policy, which may take place out of UTC, but is linked to membership of the UTC.
- **The Education Act 2011** gives the UTC the power to confiscate and search the contents of any mobile device if the Headteacher believes it contains any illegal content or material that could be used to bully or harass others.

<https://www.gov.uk/government/publications/searching-screening-and-confiscation>

- The UTC will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parents/carers of incidents of inappropriate Online Safeguarding behaviour that takes place out of UTC. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.
- **Keeping Children Safe In Education September 2025** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent UTC Standards) Regulations 2014 and the Education (Non-Maintained Special UTCs) (England) Regulations 2011. UTCs and colleges must have regard to it when carrying out their duties to safeguard and promote the welfare of children. The document contains information on what UTCs **should** do and sets out the legal duties with which UTCs and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children March 2026**.

▪ Counter-Terrorism and Security Act 2015

From 1 July 2015 all UTCs, registered early years childcare providers and registered later years childcare providers are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have “due regard to the need to prevent people from being drawn into terrorism”.

The statutory guidance on the Prevent duty summarises the requirements on UTCs and childcare providers in terms of four general themes: risk assessment, working in partnership, staff training and IT policies.

<https://www.gov.uk/government/publications/protecting-children-from-radicalisation-the-prevent-duty>

Development / Monitoring / Review of this Policy

This online safety policy has been developed by the Online Safety Group made up of:

- Principal and senior leaders
- Online Safety Lead
- Staff – including teachers, support staff, technical staff
- Governors
- Parents and carers
- Community users

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

Schedule for Development/Monitoring/Review

This online safety policy was approved by the Governing Body on:	February 2026
The implementation of this online safety policy will be monitored by:	Jessica Stevenson / Theresa Clark
Monitoring will take place at regular intervals:	Daily
The Governing Body will receive a report on the implementation of the online safety policy generated by the monitoring group (which will include anonymous details of online safety incidents) at regular intervals:	Annually
The online safety policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	February 2027
Should serious online safety incidents take place, the following external persons/agencies should be informed:	Sheffield Safeguarding Hub: 0114 273 4855 LADO AND Prevent: 0114 273 4850 lado@sheffield.gcsx.gov.uk

The UTC will monitor the impact of the policy using:

- Logs of reported incidents – on CPOMS
- Monitoring logs of internet activity (including sites visited)/filtering
- Internal monitoring data for network activity
- Surveys/questionnaires of
 - students
 - parents/carers
 - staff

Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the UTC:

Governors

Governors are responsible for the approval of the online safety policy and for reviewing the effectiveness of the policy. 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. The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Lead
- attendance at Online Safety Group meetings
- regular monitoring of online safety incident logs
- regular monitoring of filtering/change control logs
- reporting to relevant Governor's meeting

Principal and Senior Leaders

- The Principal has a duty of care for ensuring the safety (including online safety) of members of the UTC community, though the day-to-day responsibility for online safety will be delegated to the Online Safety Lead.
- The Principal 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 – included in a later section – “Responding to incidents of misuse” and relevant Local Authority disciplinary procedures).
- The Principal and Senior Leaders are responsible for ensuring 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 Principal and Senior Leaders will ensure that there is a system in place to allow for monitoring and support of those in UTC who carry out the internal online safety monitoring role. This is to provide a safety net and also support to those colleagues who take on important monitoring roles.
- The Senior Leadership Team will receive regular monitoring reports from the Online Safety Lead.

Online Safety Lead

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the UTC online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with the Local Authority
- liaises with UTC technical staff
- receives reports of online safety incidents and creates a log of incidents to inform future online safety developments,
- meets regularly with Online Safety Governor to discuss current issues, review incident logs and filtering/change control logs
- attends relevant meetings of Governors
- reports regularly to Senior Leadership Team

- Coordinates with the Online Safety Curriculum Lead * Works with the safeguarding team to ensure the curriculum is responsive to need.

Network Manager/Technical staff

Those with technical responsibilities are responsible for ensuring:

- that the UTC's technical infrastructure is secure and is not open to misuse or malicious attack
- that the UTC meets required online safety technical requirements and any Local Authority online safety policy/guidance that may apply
- that users may only access the networks and devices through a properly enforced password protection policy
- the filtering policy 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")
- that they keep up to date with online safety technical information to effectively carry out their online safety role and to inform and update others as relevant
- that the use of the networks/internet/digital technologies is regularly monitored in order that any misuse/attempted misuse can be reported to the Principal and Online Safety Lead for investigation/action/sanction
- that monitoring software/systems are implemented and updated as agreed in UTC 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 UTC online safety policy and practices
- they have read, understood and signed the staff acceptable use policy (AUP)
- they report any suspected misuse or problem to the Principal/Online Safety for investigation/action/sanction
- all digital communications with students/parents/carers should be on a professional level and only carried out using official UTC systems
- online safety issues 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 devices, cameras, etc. in lessons and other UTC activities (where allowed) and implement current policies about 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.

Designated Safeguarding Lead

Should be trained in online safety issues and be aware of the potential for serious child protection/safeguarding issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming and exploitation
- online-bullying
- Misinformation and fake news
- Radicalisation (linked to the prevent duty)

Students:

- are responsible for using the UTC digital technology systems in accordance with the student acceptable use agreement
- 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 online-bullying
- should understand the importance of adopting good online safety practice when using digital technologies out of UTC and realise that the UTC's online safety policy covers their actions out of UTC, if related to their membership of the UTC.

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 UTC will take every opportunity to help parents understand these issues through parents' evenings, newsletters, letters, website, social media and information about national/local online safety campaigns/literature. Parents/carers will be encouraged to support the UTC in promoting good online safety practice and to follow guidelines on the appropriate use of:

- digital and video images taken at UTC events.
- access to parents' sections of the website and on-line student records
- their children's personal devices in the UTC (where this is allowed)

Policy Statements

Education – Students

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

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

- A planned online safety curriculum will be provided as part of the UTC's Personal development curriculum is regularly revisited
- Key online safety messages are reinforced as part of a planned programme of assemblies and tutorial/pastoral activities including advanced ones for Computing and IT students
- Students are 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 are taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet
- Students are supported in building resilience to radicalisation by providing a safe environment for debating controversial issues and helping them to understand how they can influence and participate in decision-making. Under the Counter Terrorism and Securities Act 2015 which requires UTCs to ensure that children are safe from terrorist and extremist material on the internet
- Students should be helped to understand the need for the student acceptable use agreement and encouraged to adopt safe and responsible use both within and outside UTC

- Staff should act as good role models in their use of digital technologies, the internet and mobile devices
- 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
- Where students are allowed to freely search the internet, staff should 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 (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 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 parent/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. Parent/carers 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 UTC will therefore seek to provide information and awareness to parents and carers through:

- Curriculum activities
- Letters, newsletters, web site
- Parents/carers evenings/sessions
- High profile events/campaigns e.g. [Safer Internet Day](#)
- Reference to the relevant web sites/publications e.g. swgfl.org.uk, www.saferinternet.org.uk/, <http://www.childnet.com/parents-and-carers> (see appendix for further links/resources)

Education – The Wider Community

The UTC will provide opportunities for local community groups/members of the community to gain from the UTC'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 UTC website will provide online safety information for the wider community
- Sharing their online safety expertise/good practice with other local UTCs

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 UTC/academy online safety policy and acceptable use agreements
- It is expected that some staff will identify online safety as a training need within the performance management process
- The Online Safety Lead 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 in staff/team meetings/training sessions
- The Online Safety Lead will provide advice/guidance/training to individuals as required.

Training – Governors

Governors should take part in online safety training/awareness sessions, with particular importance for those who are members of any group involved in technology/online safety/health and safety /safeguarding. This may be offered in several ways:

- Attendance at training provided by the Local Authority or other relevant organisation (e.g. [SWGfL](#)).
- Participation in UTC training/information sessions for staff or parent/carers

Technical – infrastructure/equipment, filtering and monitoring

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

- UTC technical systems will be managed in ways that ensure that the UTC meets recommended technical requirements
- There will be regular reviews and audits of the safety and security of UTC technical systems
- Servers, wireless systems and cabling must be securely located and physical access restricted
- All users will have clearly defined access rights to UTC technical systems and devices
- All users will be provided with a username and secure password by IT Support who will keep an up-to-date record of users and their usernames. Users are responsible for the security of their username and password
- The “master/administrator” passwords for the UTC systems, used by the Network Manager must also be available to the Principal and kept in a secure place (e.g. UTC safe)
- The Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations
- 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 (see appendix for more details)
- Internet filtering/monitoring should ensure that children are safe from terrorist and extremist material when accessing the internet. Additional duties for UTCs under the Counter Terrorism and Securities Act 2015 which requires UTCs/academies to ensure that children are safe from terrorist and extremist material on the internet. (see appendix for information on “appropriate filtering”)
- The UTC has provided enhanced/differentiated user-level filtering (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc)
- UTC technical staff regularly monitor and record the activity of users on the UTC technical systems and users are made aware of this in the acceptable use agreement
- An appropriate system is in place for users to report any actual/potential technical incident/security breach to the relevant person, as agreed

- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations, mobile devices, etc. from accidental or malicious attempts which might threaten the security of the UTC systems and data. These are tested regularly. The UTC infrastructure and individual devices are protected by up-to-date virus software
- An agreed policy is in place for the provision of temporary access of “guests” (e.g. trainee teachers, supply teachers, visitors) onto the UTC systems
- An agreed policy is in place regarding the extent of personal use that users (staff/students) and their family members are allowed on UTC devices that may be used out of UTC
- An agreed policy is in place that allows staff to/forbids staff from downloading executable files and installing programmes on UTC devices
- An agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on UTC devices. Personal data cannot be sent over the internet or taken off the UTC site unless safely encrypted or otherwise secured (see UTC Personal Data Policy Template in the appendix for further detail) .

Mobile Technologies (including BYOD/BYOT)

Mobile technology devices may be UTC owned/provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising the UTC’s wireless network. The device then has access to the wider internet which may include the UTC’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 devices in a UTC context is educational. The mobile technologies policy should be consistent with and inter-related to other relevant UTC policies including but not limited to the safeguarding policy, behaviour policy, bullying policy, acceptable use policy, and policies around theft or malicious damage. Teaching about the safe and appropriate use of mobile technologies should be an integral part of the UTC’s online safety education programme.

- The UTC acceptable use agreements for staff, students and parents/carers will consider the use of mobile technologies
- The UTC allows:

UTC Devices		Personal Devices				
	UTC owned for single user	UTC owned for multiple users	Authorised device ¹	Student owned	Staff owned	Visitor owned
Allowed in UTC	Yes	Yes	Yes	Yes	Yes	Yes
Full network access	Yes	Yes	No	No	No	No
Internet only	Yes	Yes	Yes	Yes	Yes	Yes

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.

¹ Authorised device – purchased by the pupil/family through a school-organised scheme. This device may be given full access to the network as if it were owned by the school.

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 online 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 UTC 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 will be obtained before photographs of students are published on the UTC website/social media/local press
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at UTC events for their own personal use (as such use is 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 UTC policies concerning the sharing, distribution and publication of those images. Those images should only be taken on UTC 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 UTC 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
- Student's work can only be published with the permission of the student and/or parents/carers.

Data Protection

With effect from 25th May 2018, the data protection arrangements for the UK changed following the European Union General Data Protection Regulation (GDPR). As a result, UTCs are likely to be subject to greater scrutiny in their care and use of personal data. More detailed guidance is available in the appendices to this document. UTCs should ensure that they take account of policies and guidance provided by local authorities or other relevant bodies.

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation.

The UTC therefore ensure that:

- it has a Data Protection Policy
- it implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records
- it has paid the appropriate fee Information Commissioner's Office (ICO) and included details of the Data Protection Officer (DPO)

- it has appointed an appropriate Data Protection Officer (DPO) who has a high level of understanding of data protection law and is free from any conflict of interest. The UTC may also wish to appoint a Data Manager and Systems Controllers to support the DPO
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it
- the information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- it will hold only 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. The UTC should develop and implement a 'retention policy' to ensure there are clear and understood policies and routines for the deletion and disposal of data to support this. personal data held must be accurate and up to date where this is necessary for the purpose it is processed for. Have systems in place to identify inaccuracies, such as asking parent/carers to check emergency contact details at suitable intervals
- it provides staff, parents, volunteers, teenagers and older children with information about how the UTC looks after their data and what their rights are in a clear Privacy Notice (see Privacy Notice section in the appendix)
- procedures must be in place to deal with the individual rights of the data subject, e.g. one of the 8 data subject rights applicable is that of Subject Access which enables an individual to see to have a copy of the personal data held about them (subject to certain exceptions which may apply)
- data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- IT system security is ensured and regularly checked. Patches and other security essential updates are applied promptly to protect the personal data on the systems. Administrative systems are securely ring fenced from systems accessible in the classroom/to learners
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed
- it understands how to share data lawfully and safely with other relevant data controllers
- it [reports any relevant breaches to the Information Commissioner](#) within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a policy for reporting, logging, managing, investigating and learning from information risk incidents
- If a maintained UTC, it must have a Freedom of Information Policy which sets out how it will deal with FOI requests
- all staff receive data protection training at induction and appropriate refresher training thereafter. Staff undertaking particular data protection functions, such as handling requests under the individual's rights, will receive training appropriate for their function as well as the core training provided to all staff

When personal data is stored on any mobile device or removable media the:

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

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
- can recognise a possible breach, understand the need for urgency and know who to report it to within the UTC

- can help data subjects understand their rights and know how to handle a request whether verbal or written. Know who to pass it to in the UTC
- where personal data is stored or transferred on mobile or other devices (including USBs) these must be encrypted and password protected
- will not transfer any UTC personal data to personal devices except as in line with UTC policy
- access personal data sources and records 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.

Communications

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

	Staff & other adults				Students			
	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Communication Technologies								
Mobile phones may be brought to UTC		X				X		
Use of mobile phones in lessons		X				X		
Use of mobile phones in social time	X				X			
Taking photos on mobile phones/cameras			X				X	
Use of other mobile devices e.g. tablets, gaming devices	X					X		
Use of personal email addresses in UTC, or on UTC network				X				X
Use of UTC email for personal emails				X				X
Use of messaging Apps		X				X		
Use of social media			X			X		
Use of blogs		X				X		

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

- The official UTC email service may be regarded as safe and secure and is monitored. Users should be aware that email communications are monitored. Staff and students should therefore use only the UTC/academy email service to communicate with others when in UTC, or on UTC/academy systems (e.g. by remote access)
- Users must immediately report, to the nominated person – in accordance with the UTC/academy policy, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication
- Any digital communication between staff and students or parents/carers (email, social media, chat, blogs, ClassCharts etc) must be professional in tone and content. These communications may only take place on official (monitored) UTC systems. 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
- Personal information should not be posted on the UTC website and only official email addresses should be used to identify members of staff.

The UTC provides the following measures to ensure reasonable steps are in place to minimise risk of harm to students, staff and the UTC through:

- Ensuring that personal information is not published
- Training is provided including acceptable use; social media risks; checking of settings; data protection; reporting issues
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk.

UTC staff should ensure that:

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

When official UTC social media accounts are established, there should be:

- A process for approval by senior leaders
- Clear processes for the administration and monitoring of these accounts – involving at least two members of staff
- A code of behaviour for users of the accounts, including:
 - Systems for reporting and dealing with abuse and misuse
 - Understanding of how incidents may be dealt with under UTC disciplinary procedures.

Personal Use:

- Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the UTC or impacts on the UTC, it must be made clear that the member of staff is not communicating on behalf of the UTC with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon the UTC are outside the scope of this policy
- Where excessive personal use of social media in UTC is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The UTC permits reasonable and appropriate access to private social media sites.

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the UTC
- The UTC should effectively respond to social media comments made by others according to a defined policy or process

The UTC's use of social media for professional purposes will be checked regularly by the senior risk officer and designated safeguarding lead.

Dealing with unsuitable/inappropriate activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned from UTC and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are, however a range of activities which may, generally, be legal but would be inappropriate in a UTC context, either because of the age of the users or the nature of those activities.

The UTC believes that the activities referred to in the following section would be inappropriate in a UTC context and that users, as defined below, should not engage in these activities in/or outside the UTC when using UTC equipment or systems. The UTC policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978 UKSIC Responding to and managing sexting incidents and UKCIS – Sexting in UTCs and colleges					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				X	

Promotion of extremism or terrorism				X	
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the UTC or brings the UTC into disrepute				X	

Activities that might be classed as cyber-crime under the Computer Misuse Act:

- Gaining unauthorised access to UTC networks, data and files, through the use of computers/devices
- Creating or propagating computer viruses or other harmful files
- Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)
- Disable/Impair/Disrupt network functionality through the use of computers/devices
- Using penetration testing equipment (without relevant permission)

UTCs will need to decide whether these should be dealt with internally or by the police. Serious or repeat offences should be reported to the police. Under the Cyber-Prevent agenda the National Crime Agency has a remit to prevent young people becoming involved in cyber-crime and harness their activity in positive ways – further information [here](#)

Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the UTC

Revealing or publicising confidential or proprietary information (e.g. financial/personal information, databases, computer/network access codes and passwords)

Unfair usage (downloading/uploading large files that hinders others in their use of the internet)

Using UTC systems to run a private business

Infringing copyright

On-line gaming (educational)

On-line gaming (non-educational)

On-line gambling

On-line shopping/commerce

File sharing

Use of social media

Use of messaging apps

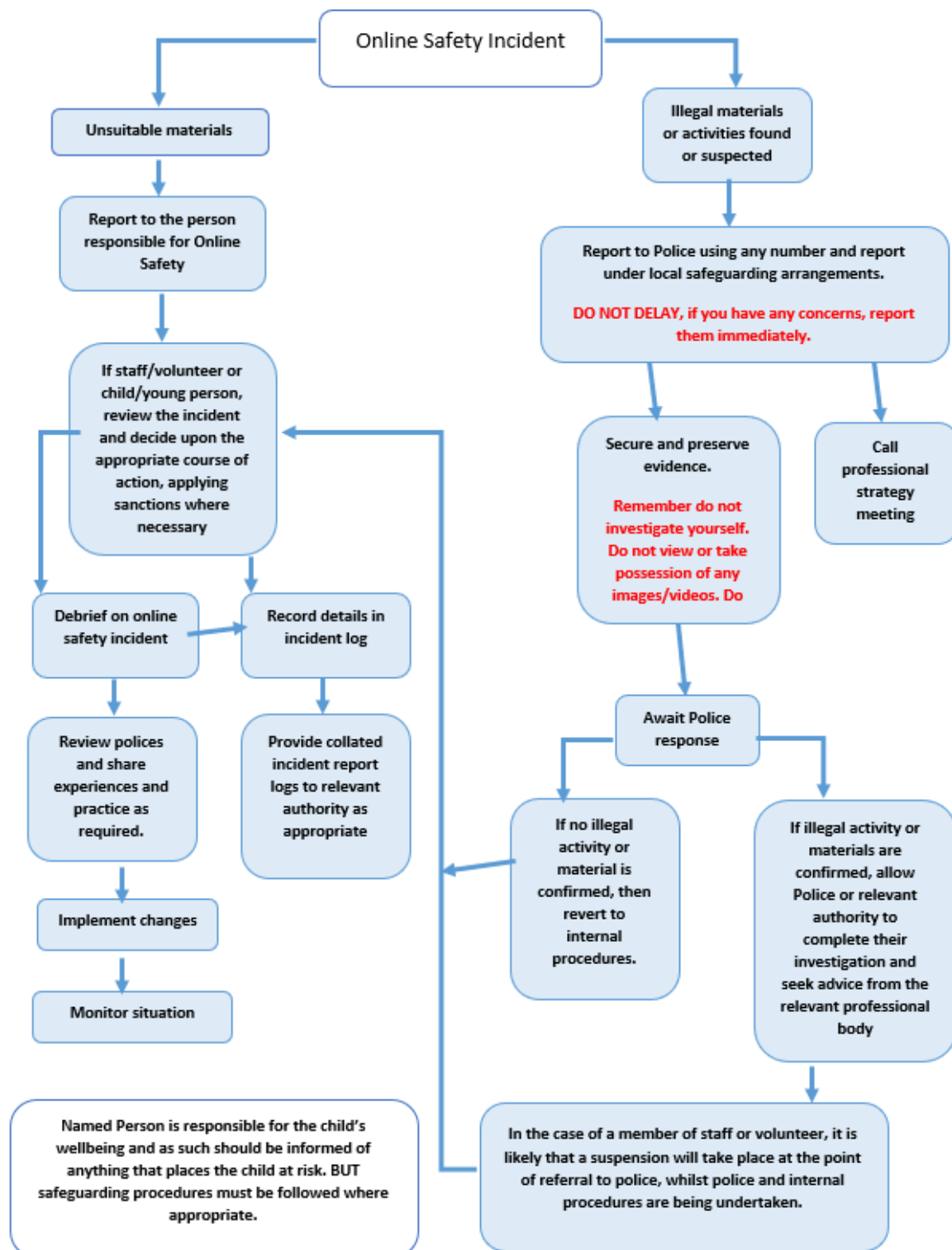
Use of video broadcasting e.g. Youtube

Responding to incidents of misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see “user actions” above).

Illegal Incidents

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



Other Incidents

It is hoped that all members of the UTC community will be responsible users of digital technologies, who understand and follow UTC policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

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

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated the group will need to judge whether this concern has substance or not. If it does, then appropriate action will be required and could include the following:
 - Internal response or discipline procedures
 - Involvement by Local Authority/Academy Group or national/local organisation (as relevant).
 - Police involvement and/or action
- If content being reviewed includes images of child abuse, then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include:
 - incidents of 'grooming' behaviour
 - the sending of obscene materials to a child
 - adult material which potentially breaches the Obscene Publications Act
 - criminally racist material
 - promotion of terrorism or extremism
 - offences under the Computer Misuse Act (see User Actions chart above)
 - other criminal conduct, activity or materials
- Isolate the computer in question as best you can. Any change to its state may hinder a later police investigation.

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

UTC actions & sanctions

It is more likely that the UTC will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the UTC community are aware that incidents have been dealt with. It is intended that incidents of misuse will be dealt with through normal behaviour/disciplinary procedures as follows:

Actions / Sanctions

Student Incidents:	Refer to Learning Manager	Refer to SLT	Refer to Safeguarding team / DSL	Refer to Principal	Refer to Police	Refer to technical support staff for action re filtering / security etc.	Inform parents / carers	Removal of network / internet access rights	Warning	Further sanction e.g. detention / exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).			X	X	X	X	X	X		X
Unauthorised use of non-educational sites during lessons	X					X	X			X
Unauthorised use of mobile phone / digital camera / other handheld device	X						X			X
Unauthorised use of social networking / instant messaging / personal email	X						X			X
Unauthorised downloading or uploading of files	X					X	X	X		X
Allowing others to access UTC network by sharing username and passwords	X					X	X	X		X
Attempting to access or accessing the UTC network, using another student's / student's account	X					X	X	X		X
Attempting to access or accessing the UTC network, using the account of a member of staff		X				X	X	X		X
Corrupting or destroying the data of other users	X					X	X	X		X
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X				X	X		X

UTC Olympic Legacy Park Online Safeguarding Policy 2025-2026

Continued infringements of the above, following previous warnings or sanctions	X	X		X		X	X	X		X
Actions which could bring the UTC into disrepute or breach the integrity of the ethos of the UTC		X		X		X	X	X		X
Using proxy sites or other means to subvert the UTC's filtering system	X	X				X	X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X	X	X			X	X		X	
Deliberately accessing or trying to access offensive or pornographic material			X	X		X	X	X		X
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection Act		X		X		X	X	X		X

Staff

Incidents:	Refer to Principal	Refer to Police	Refer to Technical Support Staff for action re filtering etc.	Refer to HR	Refer to Local Authority	Disciplinary action - suspension, warning, dismissal – add note!
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities).	X	X	X	X	X	X
Excessive or inappropriate personal use of the internet / social networking sites / instant messaging / personal email	X		X	X		X
Unauthorised downloading or uploading of files	X		X	X		X
Allowing others to access UTC network by sharing username and passwords or attempting to access or accessing the UTC network, using another person's account	X		X	X		X
Careless use of personal data e.g. holding or transferring data in an insecure manner	X		X	X		X
Deliberate actions to breach data protection or network security rules	X		X	X		X
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	X	X	X	X	X	X

Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	X	X	X	X	X	X
Using personal email / social networking / instant messaging / text messaging to carrying out digital communications with students / students	X		X	X	X	X
Actions which could compromise the staff member's professional standing	X			X		X
Actions which could bring the UTC into disrepute or breach the integrity of the ethos of the UTC	X			X		X
Using proxy sites or other means to subvert the UTC's filtering system	X		X	X		X
Accidentally accessing offensive or pornographic material and failing to report the incident	X		X	X		X
Deliberately accessing or trying to access offensive or pornographic material	X		X	X	X	X
Breaching copyright or licensing regulations	X		X	X		X
Continued infringements of the above, following previous warnings or sanctions	X			X	X	X

UTC Technical Security Policy (including filtering and passwords)

Introduction

Effective technical security depends not only on technical measures, but also on appropriate policies and procedures and on good user education and training. The UTC will be responsible for ensuring that the UTC infrastructure/network is as safe and secure as is reasonably possible and that:

- users can only access data to which they have right of access
- no user should be able to access another's files (other than that allowed for monitoring purposes within the UTC's policies).
- access to personal data is securely controlled in line with the UTC's personal data policy
- logs are maintained of access by users and of their actions while users of the system
- there is effective guidance and training for users
- there are regular reviews and audits of the safety and security of UTC computer systems
- there is oversight from senior leaders and these have impact on policy and practice.

Responsibilities

The management of technical security will be the responsibility of Network Manager

Technical Security

Policy statements

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

- UTC technical systems will be managed in ways that ensure that the UTC meets recommended technical requirements
- there will be regular reviews and audits of the safety and security of UTC technical systems
- servers, wireless systems and cabling must be securely located and physical access restricted
- appropriate security measures are in place to protect the servers, firewalls, switches, routers, wireless systems, workstations, mobile devices etc from accidental or malicious attempts which might threaten the security of the UTC systems and data
- responsibilities for the management of technical security are clearly assigned to appropriate and well-trained staff
- all users will have clearly defined access rights to UTC technical systems. Details of the access rights available to groups of users will be recorded by the network manager and will be reviewed, at least annually, by the online safety group.
- users will be made responsible for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security (*see password section below*)
- Network Manager is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations (Inadequate licencing could cause the UTC to breach the Copyright Act which could result in fines or unexpected licensing costs)
- mobile device security and management procedures are in place
- UTC technical staff regularly monitor and record the activity of users on the UTC technical systems and users are made aware of this in the acceptable use agreement.
- remote management tools are used by staff to control workstations and view users' activity
- an appropriate system is in place for users to report any actual/potential technical incident to the Online Safety Lead
- an agreed policy is in place for the provision of temporary access of "guests", (e.g. trainee teachers, supply teachers, visitors) onto the UTC system

- an agreed policy is in place regarding the downloading of executable files and the installation of programmes on UTC devices by users
- an agreed policy is in place regarding the extent of personal use that users (staff/learners) and their family members are allowed on UTC devices that may be used out of UTC
- an agreed policy is in place regarding the use of removable media (e.g. memory sticks/CDs/DVDs) by users on UTC/academy devices
- the UTC infrastructure and individual workstations are protected by up-to-date software to protect against malicious threats from viruses, worms, trojans etc.
- personal data cannot be sent over the internet or taken off the UTC/academy site unless safely encrypted or otherwise secured.

Password Security

A safe and secure username/password system is essential if the above is to be established and will apply to all UTC technical systems, including networks, devices, email and learning platform.

Policy Statements:

- These statements apply to all users.
- All UTC networks and systems will be protected by secure passwords.
- All users have clearly defined access rights to UTC technical systems and devices. Details of the access rights available to groups of users will be recorded by the Network Manager and will be reviewed, at least annually, by the online safety group (or other group).
- All users (adults and students) have responsibility for the security of their username and password, must not allow other users to access the systems using their log on details and must immediately report any suspicion or evidence that there has been a breach of security.
- Passwords must not be shared with anyone.
- All users will be provided with a username and password by the Network Manager who will keep an up-to-date record of users and their usernames.

Password requirements:

- Passwords should be long. Good practice highlights that passwords over 12 characters in length are considerably more difficult to compromise than shorter passwords. Passwords generated by using a combination of unconnected words that are over 16 characters long are extremely difficult to crack. Password length trumps any other special requirements such as uppercase/lowercase letters, number and special characters. Passwords should be easy to remember, but difficult to guess or crack.
- Passwords should be different for different accounts, to ensure that other systems are not put at risk if one is compromised and should be different for systems used inside and outside of UTC
- Passwords must not include names or any other personal information about the user that might be known by others
- Passwords must be changed on first login to the system

Learner passwords:

- Password requirements for students should increase as students' progress through UTC.
- Users will be required to change their password if it is compromised.
- Students will be taught the importance of password security, this should include how passwords are compromised, and why these password rules are important.

Notes for technical staff/teams

- Each administrator should have an individual administrator account, as well as their own user account with access levels set at an appropriate level. Consideration should also be given to using two factor authentication for such accounts.

- An administrator account password for the UTC systems should also be kept in a secure place e.g. UTC safe. This account and password should only be used to recover or revoke access. Other administrator accounts should not have the ability to delete this account.
- Any digitally stored administrator passwords should be hashed using a suitable algorithm for storing passwords (e.g. Bcrypt or Scrypt). Message Digest algorithms such as MD5, SHA1, SHA256 etc. should not be used.
- It is good practice that where passwords are used there is a user-controlled password reset process to enable independent, but secure re-entry to the system. This ensures that only the owner has knowledge of the password.
- Where user-controlled reset is not possible, passwords for new users, and replacement passwords for existing users will be allocated by the Network Manager. Good practice is that the password generated by this change process should be system generated and only known to the user. This password should be temporary, and the user should be forced to change their password on first login. The generated passwords should also be long and random.
- Where automatically generated passwords are not possible, then a good password generator should be used by the Network Manager to provide the user with their initial password. There should be a process for the secure transmission of this password to limit knowledge to the password creator and the user. The password should be temporary, and the user should be forced to change their password on the first login.
- Requests for password changes should be authenticated by the Network Manager to ensure that the new password can only be passed to the genuine user
- Suitable arrangements should be in place to provide visitors with appropriate access to systems which expires after use. (For example, your technical team may provide pre-created user/password combinations that can be allocated to visitors, recorded in a log, and deleted from the system after use.)
- In good practice, the account is “locked out” following six successive incorrect log-on attempts.
- Passwords shall not be displayed on screen and shall be securely hashed when stored (use of one-way encryption).

Training/Awareness:

Members of staff will be made aware of the UTC password policy:

- at induction
- through the UTC online safety policy and password security policy
- through the acceptable use agreement

Students will be made aware of the UTC’s password policy:

- in lessons
- through the acceptable use agreement

Audit/Monitoring/Reporting/Review:

The responsible person, the Network Manager, will ensure that full records are kept of:

- User Ids and requests for password changes
- User logons
- Security incidents related to this policy

Filtering

Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so, because the content on the web changes dynamically and new technologies are constantly being developed. It is important, therefore, to understand that filtering is only one element in a larger strategy for online safety and acceptable use.

It is important that the UTC has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this UTC.

Responsibilities

The responsibility for the management of the UTC's filtering policy will be held by the Network Manager. They will manage the UTC filtering, in line with this policy and will keep records/logs of changes and of breaches of the filtering systems.

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

- be logged in change control logs
- be reported to a second responsible person, the Business Manager:

All users have a responsibility to report immediately to DSL and Technical manager any infringements of the UTC's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

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

Policy Statements

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

- The UTC has provided enhanced/differentiated user-level filtering using the Smoothwall filtering programme (allowing different filtering levels for different ages/stages and different groups of users – staff/students etc.)
- In the event of the technical staff needing to switch off the filtering for any reason, or for any user, this must be logged and carried out by a process that is agreed by the Principal.
- Mobile devices that access the UTC internet connection (whether UTC or personal devices) will be subject to the same filtering standards as other devices on the UTC systems.
- Any filtering issues should be reported immediately to the filtering provider.
- Requests from staff for sites to be removed from the filtered list will be considered by the technical staff the Network Manager. If the request is agreed, this action will be recorded, and logs of such actions shall be reviewed regularly by the Online Safety Group.

Education/Training/Awareness

Students will be made aware of the importance of filtering systems through the Global Cultural Learning Programme. They will also be warned of the consequences of attempting to subvert the filtering system.

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

- the acceptable use agreement
- induction training
- staff meetings, briefings, Inset

Parents will be informed of the UTC's filtering policy through the acceptable use agreement and through online safety awareness sessions/newsletter etc.

Changes to the Filtering System

In this section the UTC should provide a detailed explanation of:

- how, and to whom, users may request changes to the filtering (whether this is carried out in UTC or by an external filtering provider)
- the grounds on which they may be allowed or denied (UTCs may choose to allow access to some sites e.g. social networking sites for some users, at some times, or for a limited period of time. There should be strong educational reasons for changes that are agreed).
- how a second responsible person will be involved to provide checks and balances (preferably this will be at the time of request, but could be retrospectively through inspection of records/audit of logs)
- any audit/reporting system

Users who gain access to, or have knowledge of others being able to access, sites which they feel should be filtered (or unfiltered) should report this in the first instance to the network manager via the helpdesk who will decide whether to make UTC level changes (as above).

Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The UTC will therefore monitor the activities of users on the UTC network and on UTC equipment as indicated in the UTC online safety policy and the acceptable use agreement. Monitoring will take place as follows:

Audit/Reporting

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

- the second responsible person Designated Safeguarding Lead
- Safeguarding Governor
- External Filtering provider/Local Authority/Police on request

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

Further Guidance

UTCs may wish to seek further guidance. The following is recommended:

UTCs in England (and Wales) are required *“to ensure children are safe from terrorist and extremist material when accessing the internet in UTC, including by establishing appropriate levels of filtering”* ([Revised Prevent Duty Guidance: for England and Wales, 2015](#)).

The Department for Education *‘Keeping Children Safe in Education’* requires UTCs to: *“ensure appropriate filters and appropriate monitoring systems are in place. Children should not be able to access harmful or inappropriate material from the UTC or colleges IT system”* however, UTCs will need to *“be careful that “over blocking” does not lead to unreasonable restrictions as to what children can be taught with regards to online teaching and safeguarding.”*

In response UKSIC produced guidance on – information on *“Appropriate Filtering”*

SWGfL provides a site for UTCs to test their filtering to ensure that illegal materials cannot be accessed: [SWGfL Test Filtering](#)

- The UTC accepts no responsibility for any malfunction of a device due to changes made to the device while on the UTC/academy network or whilst resolving any connectivity issues
- The UTC recommends that the devices are made easily identifiable and have a protective case to help secure them as the devices are moved around the UTC. Passcodes or PINs should be set on personal devices to aid security
- The UTC is not responsible for the day-to-day maintenance or upkeep of the users personal device such as the charging of any device, the installation of software updates or the resolution of hardware issues

- Users are expected to act responsibly, safely and respectfully in line with current acceptable use agreements, in addition;
 - Devices may not be used in tests or exams
 - Visitors should be provided with information about how and when they are permitted to use mobile technology in line with local safeguarding arrangements
 - Users are responsible for keeping their device up to date through software, security and app updates. The device is virus protected and should not be capable of passing on infections to the network
 - Users are responsible for charging their own devices and for protecting and looking after their devices while in the UTC
 - Personal devices should be charged before being brought to the UTC as the charging of personal devices is not permitted during the UTC day
 - Devices must be in silent mode on the UTC site
 - UTC devices are provided to support learning. It is expected that students will bring devices to the UTC as required.
 - Confiscation and searching (England) - the UTC has the right to take, examine and search any device that is suspected of unauthorised use, either technical or inappropriate.
 - The changing of settings (exceptions include personal settings such as font size, brightness, etc.) that would stop the device working as it was originally set up and intended to work is not permitted
 - The software/apps originally installed by the UTC must remain on the UTC owned device in usable condition and be easily accessible at all times. From time to time the UTC may add software applications for use in a particular lesson. Periodic checks of devices will be made to ensure that users have not removed required apps
 - The UTC will ensure that devices contain the necessary apps for UTC work. Apps added by the UTC will remain the property of the UTC and will not be accessible to students on authorised devices once they leave the UTC roll. Any apps bought by the user on their own account will remain theirs
 - Users should be mindful of the age limits for app purchases and use and should ensure they read the terms and conditions before use
 - Users must only photograph people with their permission. Users must only take pictures or videos that are required for a task or activity. All unnecessary images or videos will be deleted immediately
 - Devices may be used in lessons in accordance with teacher direction
 - Staff owned devices should not be used for personal purposes during teaching sessions, unless in exceptional circumstances
 - Printing from personal devices will not be possible

Social Media Policy

Social media (e.g. Facebook, Twitter, LinkedIn) is a broad term for any kind of online platform which enables people to directly interact with each other. However, some games, for example Minecraft or World of Warcraft and video sharing platforms such as You Tube have social media elements to them.

The UTC recognises the numerous benefits and opportunities which a social media presence offers. Staff, parents/carers and students are actively encouraged to find creative ways to use social media.

However, there are some risks associated with social media use, especially around the issues of safeguarding, bullying and personal reputation. This policy aims to encourage the safe use of social media by the UTC/academy, its staff, parents, carers and children.

Scope

This policy is subject to the UTC's codes of conduct and acceptable use agreements.

This policy:

- Applies to all staff and to all online communications which directly or indirectly, represent the UTC.
- Applies to such online communications posted at any time and from anywhere.
- Encourages the safe and responsible use of social media through training and education.
- Defines the monitoring of public social media activity pertaining to the UTC

The UTC respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the UTC's reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on a UTC account or using the UTC name. All professional communications are within the scope of this policy.

Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with, or impacts on, the UTC, it must be made clear that the member of staff is not communicating on behalf of the UTC with an appropriate disclaimer. Such personal communications are within the scope of this policy.

Personal communications which do not refer to or impact upon the UTC are outside the scope of this policy.

Digital communications with students are also considered. Staff may use social media to communicate with learners via a UTC social media account for teaching and learning purposes but must consider whether this is appropriate and consider the potential implications.

Organisational control

Roles & Responsibilities

- **SLT**
 - Facilitating training and guidance on Social Media use
 - Developing and implementing the Social Media policy
 - Taking a lead role in investigating any reported incidents
 - Making an initial assessment when an incident is reported and involving appropriate staff and external agencies as required
 - Receive completed applications for Social Media accounts
 - Approve account creation
- **Administrator/Moderator**
 - Create the account following SLT approval
 - Store account details, including passwords securely
 - Be involved in monitoring and contributing to the account
 - Control the process for managing an account after the lead staff member has left the organisation (closing or transferring)

- **Staff**

- Know the contents of and ensure that any use of social media is carried out in line with this and other relevant policies
- Attending appropriate training
- Regularly monitoring, updating and managing content he/she has posted via UTC accounts
- Adding an appropriate disclaimer to personal accounts when naming the UTC

Process for creating new accounts

The UTC community is encouraged to consider if a social media account will help them in their work, e.g. a history department Twitter account, or a “Friends of the UTC” Facebook page. Anyone wishing to create such an account must present a business case to the Leadership Team which covers the following points:-

- The aim of the account
- The intended audience
- How the account will be promoted
- Who will run the account (at least two staff members should be named)
- Will the account be open or private/closed

Following consideration by the SLT an application will be approved or rejected. In all cases, the SLT must be satisfied that anyone running a social media account on behalf of the UTC has read and understood this policy and received appropriate training. This also applies to anyone who is not directly employed by the UTC, including volunteers or parents.

Monitoring

UTC accounts must be monitored regularly and frequently (preferably 7 days a week, including during holidays). Any comments, queries or complaints made through those accounts must be responded to within 24 hours (or on the next working day if received at a weekend) even if the response is only to acknowledge receipt. Regular monitoring and intervention is essential in case a situation arises where bullying or any other inappropriate behaviour arises on a UTC social media account.

Behaviour

- The UTC requires that all users using social media adhere to the standard of behaviour as set out in this policy and other relevant policies
- Digital communications by staff must be professional and respectful at all times and in accordance with this policy. Staff will not use social media to infringe on the rights and privacy of others or make ill-considered comments or judgments about staff. UTC social media accounts must not be used for personal gain. Staff must ensure that confidentiality is maintained on social media even after they leave the employment of the UTC.
- Users must declare who they are in social media posts or accounts. Anonymous posts are discouraged in relation to UTC activity.
- If a journalist makes contact about posts made using social media staff must follow the UTC media policy before responding.
- Unacceptable conduct, (e.g. defamatory, discriminatory, offensive, harassing content or a breach of data protection, confidentiality, copyright) will be considered extremely seriously by the UTC and will be reported as soon as possible to a relevant senior member of staff, and escalated where appropriate.
- The use of social media by staff while at work may be monitored, in line with UTC policies. The UTC permits reasonable and appropriate access to private social media sites. However, where excessive use is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken.

- The UTC will take appropriate action in the event of breaches of the social media policy. Where conduct is found to be unacceptable, the UTC will deal with the matter internally. Where conduct is considered illegal, the UTC will report the matter to the police and other relevant external agencies, and may take action according to the disciplinary policy.

Legal considerations

- Users of social media should consider the copyright of the content they are sharing and, where necessary, should seek permission from the copyright holder before sharing.
- Users must ensure that their use of social media does not infringe upon relevant data protection laws, or breach confidentiality.

Handling abuse

- When acting on behalf of the UTC, handle offensive comments swiftly and with sensitivity.
- If a conversation turns and becomes offensive or unacceptable, UTC users should block, report or delete other users or their comments/posts and should inform the audience exactly why the action was taken.
- If you feel that you or someone else is subject to abuse by colleagues through use of a social networking site, then this action must be reported using the agreed UTC protocols.

Tone

The tone of content published on social media should be appropriate to the audience, whilst retaining appropriate levels of professional standards. Key words to consider when composing messages are:

- Engaging
- Conversational
- Informative
- Friendly (on certain platforms, e.g. Facebook)

Use of images

UTC use of images can be assumed to be acceptable, providing the following guidelines are strictly adhered to.

- Permission to use any photos or video recordings should be sought in line with the UTC's digital and video images policy. If anyone, for any reason, asks not to be filmed or photographed then their wishes should be respected
- Under no circumstances should staff share or upload student pictures online other than via UTC owned social media accounts
- Staff should exercise their professional judgement about whether an image is appropriate to share on UTC social media accounts. Students should be appropriately dressed, not be subject to ridicule and must not be on any UTC list of children whose images must not be published
- If a member of staff inadvertently takes a compromising picture which could be misconstrued or misused, they must delete it immediately.

Personal use

- **Staff**
 - Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with the UTC or impacts on the UTC, it must be made clear that the member of staff is not communicating on behalf of the UTC with an appropriate disclaimer. Such personal communications are within the scope of this policy
 - Personal communications which do not refer to or impact upon the UTC are outside the scope of this policy

- Where excessive personal use of social media in UTC is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- The UTC permits reasonable and appropriate access to private social media sites.
- **Students**
 - Staff are not permitted to follow or engage with current or prior students of the UTC on any personal social media network account
 - The UTC's education programme should enable the students to be safe and responsible users of social media
 - Students are encouraged to comment or post appropriately about the UTC. Any offensive or inappropriate comments will be resolved by the use of the UTC's behaviour policy.
- **Parents/Carers**
 - If parents/carers have access to a UTC learning platform where posting or commenting is enabled, parents/carers will be informed about acceptable use
 - The UTC has an active parent/carer education programme which supports the safe and positive use of social media. This includes information on the website
 - Parents/Carers are encouraged to comment or post appropriately about the UTC. In the event of any offensive or inappropriate comments being made, the UTC will ask the parent/carer to remove the post and invite them to discuss the issues in person. If necessary, refer parents to the UTC's complaints procedures.

Monitoring posts about the UTC

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about the UTC
- The UTC should effectively respond to social media comments made by others according to a defined policy or process.

Appendix

Managing your personal use of Social Media:

- "Nothing" on social media is truly private
- Social media can blur the lines between your professional and private life. Don't use the UTC logo and/or branding on personal accounts
- Check your settings regularly and test your privacy
- Keep an eye on your digital footprint
- Keep your personal information private
- Regularly review your connections – keep them to those you want to be connected to
- When posting online consider; Scale, Audience and Permanency of what you post
- If you want to criticise, do it politely.
- Take control of your images – do you want to be tagged in an image? What would children or parents say about you if they could see your images?
- Know how to report a problem.

Managing UTC social media accounts

The Do's

- Check with a senior leader before publishing content that may have controversial implications for the UTC
- Use a disclaimer when expressing personal views
- Make it clear who is posting content
- Use an appropriate and professional tone
- Be respectful to all parties

- Ensure you have permission to 'share' other peoples' materials and acknowledge the author
- Express opinions but do so in a balanced and measured manner
- Think before responding to comments and, when in doubt, get a second opinion
- Seek advice and report any mistakes using the UTC's reporting process
- Consider turning off tagging people in images where possible.

The Don'ts

- Don't make comments, post content or link to materials that will bring the UTC/academy into disrepute
- Don't publish confidential or commercially sensitive material
- Don't breach copyright, data protection or other relevant legislation
- Consider the appropriateness of content for any audience of UTC/academy accounts, and don't link to, embed or add potentially inappropriate content
- Don't post derogatory, defamatory, offensive, harassing or discriminatory content
- Don't use social media to air internal grievances.

Acknowledgements

With thanks to Rob Simmonds of Well Chuffed Comms (wellchuffedcomms.com) and Chelmsford College for allowing the use of their policies in the creation of this policy.