Online Safeguarding Policy

Status: Statutory

Member of Staff responsible: Principal

Associated Policies and documentation:

- Student / Student Acceptable Use Policy Agreement Template
- Staff and Volunteers Acceptable Use Policy Agreement Template
- Parents / Carers Acceptable Use Policy Agreement Template
- Child Protection/Safeguarding Policy
- Anti-bullying Policy
- Behaviour Policy
- Code of Conduct

Implementation Date: September 2020

Last Review Date: September 2023

Next review date: September 2024

Content

Rationale

Why have an Online Safeguarding Policy?

The requirement to ensure that children and young people are able to 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 peer to peer pressure, commercial advertising and adults posing as children or young adult with the intention to groom or exploit them for sexual, criminal financial or other purposes including radicalisation and extremism

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

Commerce: risks such as online gambling, inappropriate advertising, phishing and or financial scams

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 Head-teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the college site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This applies to incidents of cyber-bullying, or other Online Safeguarding incidents covered by this policy, which may take place out of school, but is linked to membership of the college.

- **The Education Act 2011** gives the college the power to confiscate and search the contents of any mobile device if the Head-teacher 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 college will identify within this policy and in the associated behaviour and anti-bullying policies, how incidents will be managed and will, where known, inform parent(s) / carers of incidents of inappropriate Online Safeguarding behaviour that takes place out of college. This includes acting within the boundaries identified in the Department for Education guidance for Searching, Screening and Confiscation.

- **Keeping Children Safe In Education September 2023** This is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011. Schools 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 schools and colleges **should** do and sets out the legal duties with which schools and colleges **must** comply. It should be read alongside statutory guidance **Working Together to Safeguard Children 2018**

- **Counter-Terrorism and Security Act 2015** From 1 July 2015 all schools, 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 schools 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 policy has been developed by the Online Safety Group made up of:

- Principal and Senior Leadership Team
- Online Safety Lead
- Staff – including Teachers, Support Staff, Technical staff
- Governors
- Parents and Carers
- Community users

Consultation with the wider whole UTC community has taken place through the distribution of the policy and collated feedback.

Schedule for Development / Monitoring / Review

Title	**UTC Derby Pride Park Online Safeguarding Policy**
Date	*22/09/2023*
Author	*S Hunt / L Kirkwood*
Monitoring will take place at regular intervals:	*Termly*
The Governing Body will receive a report on the implementation of the policy including anonymous details of any Online Safeguarding incidents at regular intervals:	*Annually*
The 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 Safeguarding or incidents that have taken place. The next anticipated review date will be:	*September 2024*
Should serious Online Safeguarding incidents take place, the following external persons / agencies should be informed:	*Derby Safeguarding Hub (MASH): 01332 642855* *LADO: 01332 642376*

The UTC will monitor the impact of the policy using:

- Logs of reported incidents
- Internal monitoring data for network activity
- Surveys / questionnaires of:
    - students / students
    - parents / carers
    - staff

Communication of the Policy

It is important to understand that any policy is only as good as the training and awareness that is packaged around it. There is no point in having an updated policy which covers all elements of Online safeguarding if no one within the UTC is aware of the policy.

UTC Derby Pride Park will communicate the most up to date policy as follows;

- The senior leadership team will be responsible for ensuring the UTC community are aware of the existence and contents of the UTC Online Safeguarding Policy and the use of any new technology as and when appropriate.
- The Online Safeguarding Policy will be provided to and discussed with all members of staff formally.
- All amendments will be published and appropriately communicated to all members of the UTC community.
- Any amendments will be discussed with the Student Council to ensure the language and vocabulary is appropriate and understandable for the policy's intended audience.
- An Online Safeguarding training programme will be established across the UTC and will include a regular review of the online safeguarding policy.
- Online Safeguarding training will be part of the Global Learning programme across the Key Stages.
- The Online Safeguarding Policy will apply when students move between education and training providers and will be communicated to all parties accordingly.
- The UTC approach to Online Safeguarding and its policy will be reinforced through the curriculum / programme of study.
- The key messages contained within the Online Safeguarding Policy will be reflected and consistent within all acceptable use policies in place within the UTC.
- We endeavour to embed Online Safeguarding messages across the curriculum whenever the internet or related technologies are used.
- The Online Safeguarding Policy will be introduced to the students at the start of each academic year.
- Safeguarding posters will be prominently displayed around the setting.

Roles and Responsibilities

The following section outlines the roles and responsibilities of individuals and groups within the UTC. The responsibilities will obviously depend on the staffing structure.

We believe that Online Safeguarding is the responsibility of the whole UTC community and **everyone** has a responsibility to ensure that **all** members of the community are able to benefit from the opportunities technology offers in learning and teaching. The following responsibilities demonstrate how each member of the community will contribute.

Governors:

Local Governors are responsible for the approval of the Online Safeguarding 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 (Child Protection / Safeguarding Governor).

The role of the Online Safety Governor will include:

- regular meetings with the Online Safety Co-ordinator
- regular monitoring of Online Safety incident logs
- regular monitoring of filtering / change control logs
- reporting to relevant Governors / Trust Board

Responsibilities of Principal and Senior Leaders:

The Principal has overall responsibility for safeguarding all members of the UTC community, though the day-to-day responsibility for Online Safeguarding will be delegated to the Online Safety Lead.

The Principal and Senior Leadership Team (SLT) are responsible for ensuring that the Online Safety Lead and other relevant staff receive suitable training to enable them to carry out their Online Safeguarding roles and to train other colleagues when necessary.

- The Principal and SLT will ensure that there is a mechanism in place to allow for monitoring and support of those in UTC who carry out the internal Online Safeguarding role. This provision provides a safety net and supports those colleagues who take on important monitoring roles.
- The SLT will receive monitoring reports from the Online Safety Lead.
- The Principal and SLT will ensure that everyone is aware of procedures to be followed in the event of a serious Online Safeguarding incident (see flow chart on dealing with Online Safety incidents included in a later section) and relevant disciplinary procedures.
- The Principal and SLT receive update reports of any incidents from the Online Safeguarding / Safeguarding team.

Responsibilities of the Online Safeguarding Team

- To ensure that the UTC Online Safeguarding Policy is current and relevant.
- To ensure that the UTC Online Safeguarding Policy is systematically reviewed at agreed time intervals.
- To ensure that UTC Acceptable Use Policies are appropriate for the intended audience.
- To promote to all members of the UTC community the safe use of the internet and any technologies deployed within UTC.

Responsibilities of the Online Safeguarding Lead

- To promote an awareness and commitment to Online Safeguarding throughout the UTC.
- To be the first point of contact in the UTC on all Online Safeguarding matters.
- To take day-to-day responsibility for Online Safeguarding within the UTC and to have a leading role in establishing and reviewing the UTC Online Safeguarding policies and procedures.
- To lead the UTC Online Safeguarding Team.

- To have regular contact with other Online Safeguarding committees, e.g. Safeguarding Children Board
- To communicate regularly with UTC technical staff.
- To communicate regularly with the designated Online Safeguarding Governor.
- To communicate regularly with the SLT.
- To create and maintain Online Safeguarding Policies and procedures.
- To develop an understanding of current Online Safeguarding issues, guidance and appropriate legislation.
- To ensure that all members of staff receive an appropriate level of training in Online Safeguarding issues.
- To ensure that Online Safeguarding education is embedded across the curriculum.
- To ensure that Online Safeguarding is promoted to parents and carers.
- To liaise with the local authority, the Local Safeguarding Children Board and other relevant agencies as appropriate.
- To monitor and report on Online Safeguarding issues to the Online Safeguarding group and the senior leadership team as appropriate.
- To ensure that all staff are aware of the procedures that need to be followed in the event of an Online Safeguarding incident.
- To ensure that Online Safeguarding incidents are logged and addressed in a timely fashion by the safeguarding team

Responsibilities of the Teaching and Support Staff

- To understand, contribute to and promote the UTC's Online Safeguarding policies and guidance.
- To understand and adhere to the UTC Staff Acceptable Use Policy.
- To report any suspected misuse or problem to the Online Safeguarding Lead.
- To develop and maintain an awareness of current Online Safeguarding issues and guidance including online exploitation, radicalisation and extremism, bullying, sexting etc.
- To model safe and responsible behaviours in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through UTC based systems, **NEVER** through personal mechanisms, e.g. email, text, mobile phones, social media etc.
- To embed Online Safeguarding messages in learning activities across all areas of the curriculum.
- To supervise and guide students carefully when engaged in learning activities involving technology.
- To ensure that students are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws.
- To be aware of Online Safeguarding issues related to the use of mobile phones, cameras and handheld devices.
- To understand and be aware of incident-reporting mechanisms within the UTC.
- To maintain a professional level of conduct in personal use of technology at all times.
- Ensure that sensitive and personal data is kept secure at all times by using only approved and encrypted data storage and by transferring data through secure communication systems.

Responsibilities of Technical Staff

- To understand, contribute to and help promote the UTC's Online Safeguarding policies and guidance.
- To understand and adhere to the UTC Staff Acceptable Use Policy.
- To report any Online Safeguarding related issues that come to your attention to the Online Safeguarding coordinator/Designated Safeguarding Lead or deputies in the case of absence.
- To develop and maintain an awareness of current Online Safeguarding issues, legislation and guidance relevant to their work such as the Prevent Duty.
- To maintain a professional level of conduct in your personal use of technology at all times.
- To support the UTC in providing a safe technical infrastructure to support learning and teaching.
- To ensure that access to the UTC network is only through an authorised, restricted mechanism.
- To ensure that provision exists for misuse detection and malicious attack.
- To take responsibility for the security of the UTC ICT system.
- To liaise with the senior management team, local authority and other appropriate people and organisations on technical issues.
- To document all technical procedures and review them for accuracy at appropriate intervals.
- To restrict all administrator level accounts appropriately.
- To ensure that access controls exist to protect personal and sensitive information held on UTC-owned devices.
- To ensure that appropriate physical access controls exist to control access to information systems and telecommunications equipment situated within UTC.
- To ensure that appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster.
- To ensure that controls and procedures exist so that access to UTC-owned software assets is restricted.

Protecting the professional identity of all staff, Governors, work placement students and volunteers

This section covers an area of professional concern that has become more relevant in recent years. The appendix to this document includes references to some important guidance – in particular the "Guidance for Safer Working Practice for Adults who work with Children and Young People".

This applies to any adult, but particularly those working with children and young people (paid or unpaid) within the UTC. Consideration should be given to how the online behaviour of staff may affect their own safety and reputation and that of the UTC.

Communication between adults and between children / young people and adults, by whatever method, should be transparent and take place within clear and explicit boundaries. This includes the wider use of technology such as mobile phones, text messaging, social networks, e-mails, digital cameras, videos, web-cams, websites, forums and blogs.

When using digital communications, staff, governors and volunteers should:

- only make contact with children and young people for professional reasons and in accordance with the policies and professional guidance of the UTC.
- not share any personal information with a child or young person e.g. should not give their personal contact details to children and young people including e-mail, home or mobile telephone numbers.
- not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role, or if the child is at immediate risk of harm.
- Not send or accept a friend request from the child/young person or parent/carers on social networks.
- be aware of and use the appropriate reporting routes available to them if they suspect any of their personal details have been compromised.
- ensure that all communications are transparent and open to scrutiny.
- be careful in their communications with children, parent/carers so as to avoid any possible misinterpretation.
- ensure that if they have a personal social networking profile, details are not shared with children and young people in their care or parents/carers (making every effort to keep personal and professional online lives separate).
- not post information online that could bring the UTC into disrepute.
- be aware of the sanctions that may be applied for breaches of policy related to professional conduct.

Responsibilities of the Designated Safeguarding Lead

- To understand the issues surrounding the sharing of personal or sensitive information and to ensure that personal data is protected in accordance with the Data Protection Act 1998.
- To understand the risks and dangers regarding access to inappropriate online contact with adults and strangers.
- To be aware of potential or actual incidents involving the grooming of children and young people in relation to sexual exploitation, radicalisation and extremism.
- To be aware of and understand online bullying and the use of social media and online gaming for this purpose.

It is important to emphasise that these are child protection issues not technical issues and that the technology provides additional means for child protection issues to develop. Some UTCs may choose to combine the role of Designated Safeguarding Lead and Online Safety Officer.

Responsibilities of Students

- To read, understand and adhere to the UTC Student Acceptable Use Policy.
- To help and support the UTC in the creation of Online Safeguarding policies and practices and to adhere to those the UTC creates.
- To know and understand UTC policies on the use of digital technologies including mobile phones, digital cameras and any other personal devices.
- To know and understand UTC policies on the use of mobile phones in the UTC.
- To know and understand UTC policies regarding online bullying.

- To take responsibility for learning about the benefits and risks of using the internet and other technologies safely both in the UTC and at home.
- To be fully aware of research skills and of legal issues relating to electronic content such as copyright laws.
- To take responsibility for each other's safe and responsible use of technology in the UTC and at home, including judging the potential risks such as online exploitation, radicalisation, sexting and online bullying.
- To ensure they respect the feelings, rights, values and intellectual property of others in their use of technology in the UTC and at home.
- To understand what action they should take if they feel worried, uncomfortable, vulnerable or at risk while using technology in the UTC and at home, or if they know of someone who this is happening to.
- To understand the importance of reporting abuse, misuse or access to inappropriate materials and to be fully aware of the incident-reporting mechanisms that exists within the UTC.
- To discuss Online Safeguarding issues with family and friends in an open and honest way.

Responsibilities of Parents / Carers

- To help and support the UTC in promoting Online Safeguarding.
- To read, understand and promote the UTC's Online Safeguarding Policy and the UTC / Student Acceptable Use Policy with their children.
- To take responsibility for learning about the benefits and risks of using the internet and other technologies that their children use in the UTC and at home.
- To take responsibility for their own awareness and learning in relation to the opportunities and risks posed by new and emerging technologies.
- To discuss Online Safeguarding concerns with their children, be aware of what content, websites and Apps they are using, apply appropriate parental controls and ensure they behave safely and responsibly when using technology.
- To model safe and responsible behaviours in their own use of technology and social media.
- To consult with the UTC if they have any concerns about their children's use of the internet and digital technology.
- To agree to and sign the acceptable use agreement which clearly sets out the use of photographic and video images outside the UTC.

To sign a acceptable use agreement containing the following statements:

- We will support the UTC approach to online safety and not deliberately upload or add any images, sounds or text that could upset or offend any member of the UTC community.
- We will support the UTC's Online Safeguarding Policy.
- Images taken of students at UTC events will be for personal use only and not uploaded or shared via the internet.
- Parents may take photographs at UTC events: however, they must ensure that any images or videos taken involving children other than their own are for personal use and will not be published on the internet including social networking sites.
- Parents and carers are asked to read through and sign acceptable use agreements on behalf of their children on admission to the UTC.

- Parents and carers are required to give written consent for the use of any images of their children in a variety of different circumstances.

Example:

UTC DERBY PRIDE PARK

UTC SHEFFIELD MAKING THE FUTURE

Data Collection Form

Legal Last Name:		**Legal First Name(s):**	
Preferred Last Name:		**Preferred First Name:**	
Date of Birth:		**Gender:**	

Address:	
Town/City:	
Postcode:	
Post 16 students only please provide your mobile number:	

Previous School:		**Year Group:**	
Does the child have Special Educational Needs and/or a disability: YES / NO			
If yes, please state			

Contact information:
Please give details of all persons **who have parental responsibility** and anyone else you wish to be contacted in an emergency. The first contact should be who the student lives with and an **email address must be provided**.

Title:	**Full Name:**
Relationship to student:	**Parental responsibility: Yes / No**
Address:	
Email address:	**Mobile phone number:**
Home phone number:	**Work phone number:**

If the second contact has parental responsibility but they do not live with the child, do they wish to receive correspondence regarding their child's progress? **Yes / No** (Please provide email address)

Title:	**Full Name**
Relationship to student:	**Parental responsibility: Yes / No**

Address:	
Email address:	**Mobile phone number:**
Home phone number:	**Work phone number:**

Title:	**Full Name:**
Relationship to student:	
Address:	
Email address:	**Mobile phone number:**
Home phone number:	**Work phone number:**

Medical Information

Doctor's Name:	**Medical Practice:**
Address:	
Telephone number:	
Medical conditions: **Medication details:** **Dietary requirements:**	

Additional Information

Ethnicity
First Language:
Which mode(s) of transport will your child use on their journey to the UTC? (this information is voluntary):

Data Protection Act 2018: The Trust is registered with the Information Commissioners Office for holding personal data. The Trust has a duty to protect this information and we will not share this data unless there is a legal basis to do so or we have consent. The Trust is required to share some of the data for example with the Local Authority and with the DfE – please see the privacy notices for more information.

Parent's signature: _____ **Date:** _____

Student's signature: _____ **Date**: _____

Parental Consent Form

Please complete and return to admin reception at UTC Derby Pride Park with the data collection form. If we need more specific consent we will ask for the individual occurrence.

Child's Name: _____ **Year Gp:** _____

Please indicate your consent by placing a tick in the Yes or No box

	Yes	No
*Photographs displayed in UTC		
*Photographs used in UTC publicity material e.g. website, media publications, prospectus		
*Photographs used in material by the Baker Dearing Trust		
Sex Education		
UTC trips within local area		

* **Images will only be used on new materials for up to three years but older images may be used for longer**

Do you give your consent to let your child leave the UTC due to Early Closure without contacting you for permission? E.g. bad weather/exceptional circumstances (please tick one box only)

In the event of the UTC needing to close early due to bad weather or other exceptional circumstances what contact do you require?
[Please select one option only]

	Yes	Initial or Signature
I consent to allow the student to leave without contacting parent for permission		
I consent to allow the student to leave without contacting parent for permission but only together with their sibling/s		
The UTC must contact parent or other Emergency Contact for permission for student to leave		

This consent form will remain in place whilst your child is at the UTC – if you or your child wishes to withdraw consent at any time please contact derbyadmin@utcderby.org.uk

Signed by parent …….. Date ……

Signed by student …… Date ……

Responsibilities of Other Community/ External Users

Community Users who access the UTC ICT systems / website / shared drives as part of the Extended UTC provision will be expected to sign a Community User AUP before being provided with access to UTC systems.

- Any external users/organisations will sign an Acceptable Use Policy (AUP) prior to using any equipment or the internet within the UTC.
- The UTC will provide an Acceptable Use Policy for any guest who needs to access the UTC computer system or internet on UTC grounds.
- The UTC will ensure that appropriate levels of supervision, filtering and monitoring exist when external users/organisations make use of the internet and ICT equipment within the UTC.

Education

Students

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

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

- A planned Online Safety curriculum will be provided as part of the UTC's Global Cultural Learning curriculum and other lessons and should be regularly revisited.
- Key Online Safety messages will be reinforced as part of a planned programme of assemblies and tutorial / pastoral activities, including promoting Safer Internet Day each year.
- Students will be 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 will be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet.
- We will discuss, remind or raise relevant Online Safety messages with students routinely wherever suitable opportunities arise during all lessons; including the need to protect personal information, consider the consequences their actions may have on others, the need to check the accuracy and validity of information they use and the need to respect and acknowledge ownership of digital materials.
- Any internet use will be carefully planned to ensure that it is age appropriate and supports the learning objectives for specific curriculum areas.
- Students will be taught how to use a range of age-appropriate online tools in a safe and effective way.
- We will remind students about their responsibilities through an end-user Acceptable Use Policy which they will sign, it will be displayed throughout the UTC and will be displayed when a user logs onto the network.
- Staff will model safe and responsible behaviour in their own use of technology during lessons.

- It is accepted that from time to time, for good educational reasons, students may need to research topics (e.g. racism, drugs, discrimination etc.) that would normally result in internet searches being blocked. In such a situation, staff can request that (a designated person) can instruct technical staff to temporarily, or permanently, 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.
- 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.
- Students will be reminded of what to do if they come across unsuitable content.
- Students will be taught about the impact of online bullying and know how to seek help if they are affected by any form of bullying.
- Students will be made aware of where to report, seek advice or help if they experience problems when using the internet and related technologies; e.g. parent or carer, teacher or trusted staff member, or an organisation such as Childline or the CEOP report abuse button.

All Staff (including Governors)

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:

- All staff will receive regular information and Online Safeguarding training through a planned programme of (termly staff meetings / annual updates etc including directed training).
- All new staff will receive Online Safety information and guidance as part of the induction process, ensuring that they fully understand the Online Safeguarding policy and Acceptable Use Policies.
- All staff will be made aware of individual responsibilities relating to the Online Safeguarding of children and know what to do in the event of misuse of technology by any member of the UTC community.
- This Online Safeguarding policy and its updates will be presented to and discussed by staff in staff / team meetings / INSET days etc.
- An audit of the Online Safety training needs of all staff will be carried out regularly.
- The Online Safety Lead will provide advice, guidance and training as required.

Parents/Carers

Parents / Carers play a crucial role in ensuring that their children understand the need to use the internet and mobile devices in a safe and responsible way and in promoting the positive use of the internet and social media. Many have only a limited understanding of Online Safety risks and issues, yet it is essential they are involved in the Online Safety education of their children and in the monitoring / regulation of the children's on-line behaviours. Parents may under-estimate 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, UTC web site
- Parents / Carers evenings

- High profile events / campaigns e.g. Safer Internet Day
- Reference to the relevant web sites / publications

Training – Governors

Governors should take part in Online Safety training / awareness sessions, with particular importance for those who are members of any sub-committee involved in technology / Online Safety / health and safety / child protection. This may be offered in a number of ways:

- Attendance at training provided by the Safeguarding Children Board / Local Authority / National Governors Association / or other relevant organisation
- Participation in UTC training / information sessions for staff or parents (this may include attendance at assemblies / lessons)
- Directed training through Educare

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.

Use of digital and video images

The development of digital imaging technologies has created significant benefits to teaching and learning, allowing staff and students instant use of images that they have uploaded themselves or downloaded from the internet. However, everyone needs to be aware of the potential risks associated with sharing images and with posting digital images on the internet. Those images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. The UTC will inform and educate users about these risks and their legal responsibilities and will implement policies to reduce the likelihood of the potential for harm.

Careful consideration must be given by the Senior Leadership Team regarding the use and storage of digital content and their legal and safeguarding obligations. **The SSCB document 'The Use of Cameras and Images within Educational Settings and on Social Media'**

(https://www.kelsi.org.uk/__data/assets/pdf_file/0020/81209/Image-Use-Policy-guidance-and-template.pdf)

gives best practice guidance in the use of all types of images, including CCTV, to ensure compliance to the Data Protection Act 1998 and other legislation. There are templates for a policy and other supporting documents such as consent forms. **It is important that written consent is gained from students and staff** to use their image and must include how it will be used i.e. Social Media, website, newsletters etc. Similarly, consent must be gained from any others who are the subject of the image prior to publication. Not gaining written consent prior to publication could result in legal action.

- When using digital images, staff will inform and educate students about the risks and current law associated with the taking, sharing, use, publication and distribution of images. In particular, they should recognise the risks attached to publishing inappropriate images on the internet or distributing through mobile technology.

- Staff are allowed to take digital / video images to support educational aims or promote celebrations and achievements, 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, including mobile phones, 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 individual 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. Staff will be aware of those students where publication of their image may put them at risk.
- Students' full names will not be used in association with photographs.
- Written permission from parent(s) or carers will be obtained before photographs of students are published on the UTC website. Permission from secondary age students should also be sought (may be covered as part of the AUP signed by parents or carers at the start of the year see Parents / Carers AUP Agreement in the appendix.
- Student's work can only be published with the permission of the student and parent(s) or carers.
- When searching for images, video or sound clips, students will be taught about copyright and acknowledging ownership.

Managing ICT systems and access: Technical infrastructure, equipment, filtering and monitoring

- The UTC will be responsible for ensuring that access to the ICT systems is as safe and secure as reasonably possible and meets recommended technical requirements.
- The Governing body will ensure that the UTC has appropriate filtering and monitoring systems in place. The Governing body will regularly review their effectiveness.
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts, which might threaten the security of the UTC systems and data. These are tested regularly.
- The network is protected externally via the UTC Firewall system and the whole network is within the Derby Schools network that will also use external Firewalls.
- The internal network & workstations are separated into VLANs with appropriate access control lists restricting traffic to the systems and networks explicitly allowed in the lists.
- Servers are administered by the Network Manager. All Servers and Workstations are protected with industry standard Antivirus software.
- The Wireless system was installed and configure by the manufacturer to the current industry specification at the time of installation. All devices on the internal network are authenticated against a radius server and BYOD/Guest devices are issued a PPSK with a length above the current recommended safe length.
- The infrastructure and appropriate hardware are protected by active, up to date virus software.
- There will be regular reviews and audits of the safety and security of technical systems.
- 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 (Inadequate licencing could cause the UTC to breach the Copyright Act which could result in fines or unexpected licensing costs).

- Servers and other key hardware or infrastructure will be located securely with only appropriate staff permitted access.
- Servers, workstations and other hardware and software will be kept updated as appropriate.
- All users will have clearly defined access rights to UTC technical systems and devices.
- The UTC will agree which users should and should not have internet access and the appropriate level of access and supervision they should receive.
- At Key Stage 3 (and above), students will have an individual user account provided by IT Support with an appropriate password which will be kept secure, in line with the student Acceptable Use Policy. They will ensure they log out after each session.
- Members of staff will access the internet using an individual ID and password, which they will keep secure. They will ensure that they log out after each session and not allow students to access the internet through their ID and password. They will abide by the staff AUP at all times.
- An appropriate system is in place (or users to report any actual / potential technical incident / security breach to IT support, the Network Manager, Business & Operations Director and Data Protection Officer).
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g. trainee teachers, supply teachers, visitors) onto UTC systems (see information on BYOD for further information.
- An agreed policy is in place (Acceptable Usage Policies) regarding the extent of personal use that users (staff / students / community users) and their family members are allowed on UTC devices that may be used out of UTC.
- An agreed policy is in place (Acceptable Usage Policies) that allows staff to / forbids staff from downloading executable files and installing programmes on UTC devices.
- An agreed policy is in place (Acceptable Usage Policies) 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 Data Protection and Security Section for further details). In addition, an appendix is signed by staff detailing the restricted the use of removable media.

Bring Your Own Device (BYOD)

Guidance for BYOD:

- The UTC has a set of clear expectations and responsibilities for all users
- The UTC adheres to the Data Protection Act principles
- All users are provided with and accept the Acceptable Use Agreement
- All network systems are secure and access for users is differentiated. Where possible these devices will be covered by the UTC's / academy's normal filtering systems, while being used on the premises
- All users will are issued a personal PPSK which is used instead of a username and password
- Mandatory training is undertaken for all staff
- Students receive training and guidance on the use of personal devices
- Regular audits and monitoring of usage will take place to ensure compliance
- Any device loss, damage or theft will be reported as stated in the incident management process

- Any inappropriate content brought into UTC on a personally-owned device, will be deleted or the device will be confiscated through the incident management process and the appropriate staff in UTC informed. Where necessary this may involve escalation to the police/social services.

Filtering internet access

- The UTC uses a filtered internet service. The filtering system is provided by Smoothwall.
- The UTC's internet provision will include filtering appropriate to the age and maturity of students.
- The UTC will always be proactive regarding the nature of content that can be viewed, sent or received through the UTC's internet provision.
- The UTC will ensure that the filtering system will block extremist content and protect against radicalisation in compliance with the Prevent Duty, Counter-Terrorism and Security Act 2015.
- The UTC will have a clearly defined procedure for reporting breaches of filtering. All staff and students will be aware of this procedure by reading and signing the Acceptable Use Policy and by attending the appropriate awareness training.
- If users discover a website with inappropriate content, this should be reported to a member of staff who will inform the Online Safety Lead. All incidents will be documented.
- If users discover a website with potentially illegal content, this should be reported immediately to the Online Safety Lead.
- The UTC will report such incidents to appropriate agencies including the filtering provider, the local authority, CEOP or the Internet Watch Foundation IWF.
- The UTC will regularly review the filtering product for its effectiveness.
- The UTC filtering system will block all sites on the Internet Watch Foundation list and Government Prevent block list and this will be kept updated.
- Any amendments to the UTC filtering policy or block-and-allow lists will be checked and assessed prior to being released or blocked.
- Students will be taught to assess content as their internet usage skills develop.
- Students will use age-appropriate tools to research internet content.
- The evaluation of online content materials is a part of teaching and learning in every subject and will be viewed as a whole-UTC requirement across the curriculum.

With regards to the filtering and monitoring standards, the UTC will:

- Identify and assign roles and responsibilities to manage filtering and monitoring systems
- Review filtering and monitoring provision at least annually
- Block harmful and inappropriate content without unreasonably impacting teaching and learning
- Have effective monitoring strategies in place that meet their safeguarding needs

Passwords

Passwords are an important aspect of computer security. They are the front line of authentication for the protection of user accounts and their associated access to ICT equipment and resources. A poorly chosen password may result in the compromise of a student's work, sensitive information regarding students or staff being lost or stolen or the UTC network being infected or attacked.

The UTC has a responsibility to ensure that all elements of the UTC infrastructure and network equipment are as safe and secure as possible. All staff and student access to UTC-owned equipment and information assets should be controlled through the use of appropriate username and password policies.

It is important that all students and staff have an awareness of how to construct a complex and secure password as well as understanding the security implications of not protecting the password once selected. A secure and robust username and password convention exists for all system access. (Email, network access, UTC management information system).

- All staff will have a unique, individually named user account and password for access to ICT equipment and information systems.
- All information systems require end users to change their password at first log on.
- Users will be prompted to change their passwords every 90 days or at any time that they feel their password may have been compromised.
- Users should change their passwords whenever there is any indication of possible system or password compromise.
- All staff and students have a responsibility for the security of their username and password. Users 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.
- All staff and students will have appropriate awareness training on protecting access to their personal username and passwords for ICT access.
- All staff and students will sign an Acceptable Use Policy prior to being given access to ICT systems which clearly sets out appropriate behaviour for protecting access to username and passwords, e.g.
    - Do not write down system passwords.
    - Only disclose your personal password to authorised ICT support staff when necessary and never to anyone else. Ensure that all personal passwords that have been disclosed are changed as soon as possible.
    - Always use your own personal passwords to access computer based services, never share these with other users.
    - Make sure you enter your personal passwords each time you log-on. Do not include passwords in any automated logon procedures.
    - Never save system-based usernames and passwords within an internet browser.
    - Always use a different password on each system, never reuse passwords.
- All access to UTC information assets will be controlled via username and password.
- No user should be able to access another user's files unless delegated permission has been granted.
- Access to personal data is securely controlled in line with the UTC's personal data policy.
- The UTC maintains a log of all accesses by users and of their activities while using the system.
- Passwords should comply with current accepted complexity recommendations.

Management of assets

All UTCs have both software and hardware assets for both teaching and learning and administrative purposes. All equipment and software comes at a cost to the UTC and should therefore be controlled and documented appropriately.

All ICT-related assets are recorded in an inventory (this could be on a spreadsheet), including any software licenses held by the setting as this will give an audit trail. It is important that there are no breaches to the licensing terms and conditions of the software used as this could result in

prosecution.

Settings should also be aware that any old hardware such as laptops, PCs, servers and removable media (memory sticks) needs to be formatted prior to disposal to ensure no sensitive or personal data remains on old hardware.

- Details of all UTC-owned hardware is entered into the main Asset system (Asset Performer Online). Where possible Servers and workstations have their asset information entered into the BIOS but this is manufacturer dependent. One of the IT Configuration systems collects all the hardware details (including BIOS information) regularly during inventory cycles. This system is independent of the Asset system.
- Details of all UTC-owned software will be recorded in a software inventory. The majority licensing is provided via online portals that the software manufactures maintain and IT login with provided credentials. Any licensing that is not provided this way is stored on the IT Support network drive with very restricted access.
- All redundant ICT equipment will be disposed of through an authorised agency. This will include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.
- All redundant ICT equipment that may have held personal data will have the storage media overwritten multiple times to ensure the data is irretrievably destroyed. Alternatively, if the storage media has failed, it will be physically destroyed. The UTC will only use authorised companies who will supply a written guarantee that this will happen.
- Disposal of any ICT equipment will conform to The Waste Electrical and Electronic Equipment Regulations 2006 and/or The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007. Further information can be found on the Environment Agency website.

Data Protection

Personal Data

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

- Personal information about children / young people, members of staff / volunteers / students and parents / carers e.g. names, addresses, contact details, legal guardianship / contact details, health records, disciplinary records
- Professional records e.g. employment history, taxation and national insurance records, appraisal records and references
- Any other information that might be disclosed by mothers and fathers / carers or by other agencies working with families

The General Data Protection Regulation (GDPR) 2018 requires every organisation processing personal data to notify with the Information Commissioner's Office, unless they are exempt.

Settings that work with children and young people are likely to be under greater scrutiny in their care and use of personal data, following high profile incidents. In May 2018, the Information Commissioners Office introduced a new fine of up to €20 million, or 4% annual global turnover – whichever is greater, for breaches of information security for both public and private sector organisations.

All UTCs must understand the implications of not securing the information assets they hold and should look to appoint a Senior Information Risk Officer (SIRO). This role may well be combined with the UTCs Data Protection Officer and, where appropriate, Information Asset Owners (IAO).

Cloud Computing

When a user network account is created an Office 365 account will be generated and linked to enable access to cloud services such as Email, OneDrive, Office Online etc. The minimum amount of information required to create an account is sent to the Microsoft servers in compliance with their data protection policy.

The Department of Education has published advice and information regarding Cloud software services and the Data Protection Act.

https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Senior Information Risk Owner (SIRO)

The Senior Information Risk Owner is the Business & Operations Director who is familiar with information risks and the organisation's response. They have the following responsibilities:

- They own the information risk policy and risk assessment
- They appoint the information asset owners (IAOs)
- They act as an advocate for information risk management

The Office of Public Sector Information has produced a publication 'Managing Information Risk' to support SIROs in their role.

Information Asset Owner (IAO)

The UTC Information Asset Owner is the Business & Operations Director. The role of the IAO is to understand:

- What information is held and for what purposes
- How information will be amended or added to over time
- Who has access to the data and why
- How information is retained and disposed of

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

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

The UTC will:-

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.
- Use personal data only on secure password protected computers and other devices, ensuring that they are properly "logged-off" at the end of any session in which they are using personal data or their computer is locked when left unattended.
- Transfer data using encryption and secure password protected devices.
- When personal data is stored on any portable computer system, USB stick or any other removable media:
    - the data must be encrypted and password protected
    - the device must be password protected
    - the device must offer approved virus and malware checking software
    - the data must be securely deleted from the device, in line with UTC policy once it has been transferred or its use is complete.

- The UTC has established an information-handling procedure and assessed the risks involved with handling and controlling access to all levels of information within the UTC.
- The UTC has deployed appropriate technical controls to minimise the risk of data loss or breaches.
- All access to personal or sensitive information owned by the UTC will be controlled appropriately through technical and non-technical access controls.
- Users should be vigilant when accessing sensitive or personal information on screen to ensure that no one else, who may be unauthorised, can read the information.
- All access to information systems should be controlled via a suitably complex password.
- Any access to personal and sensitive information should be assessed and granted by the SIRO and the applicable IAO.
- All access to the UTC information management system will be on a need-to-know or least privilege basis. All access should be granted through the SIRO or IAO.
- All information on UTC servers shall be accessed through a controlled mechanism, with file permissions allocated and assessed on a need to know/ least privilege basis. All access should be granted through the SIRO or IAO.
- Staff and students will not leave personal and sensitive printed documents on printers within public areas of the UTC.
- All physical information will be stored in controlled access areas.
- All communications involving personal or sensitive information (email, fax or post) should be appropriately secured.
- All devices taken off site, e.g. laptops, tablets, removable media or phones, will be secured in accordance with the UTC's information-handling procedures and, for example, not left in cars or insecure locations.

The UTC does not allow the use of removable storage devices unless in exceptional circumstance. Devices in the UTC are blocked from accessing removable storage devices and special requests must be actions by the Network manager.

Secure Transfer Process

If you are transmitting sensitive information or personal data e.g. by email or fax it must be transferred by a secure method so it is protected from unauthorised access.

Email

It is advisable not to use public email accounts for sending and receiving sensitive or personal data.

DO NOT include personal or sensitive information within the email itself, as the information sent should be by a secure method. This can be done by creating a document (e.g. Word document) and then encrypting the document and sending it as an attachment with the email.

Encryption makes a file non-readable to anyone who does not have the password to open it, therefore, it reduces the risk of unauthorised people having access to the information and protects staff from breaching the law.

Communication Technologies

This is an area of rapidly developing technologies and uses. The table below details the technologies allowed by various members of the UTC community. A wide range of rapidly developing communications technologies has the potential to enhance learning.

	Staff & other adults			**Students / Students**				
Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
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. Staff and students should therefore use only the UTC email service to communicate with others when in UTC, or on UTC systems (e.g. by remote access).
- Users need to be aware that email communications may be monitored.
- Users must immediately report, to the nominated person, in accordance with the UTC policy, the receipt of any email that makes them feel uncomfortable, is offensive, threatening or bullying in nature and must not respond to any such email.
- Any agreed channel of digital communication between staff, students or parents / carers must be professional in tone and content.

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 ICT 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 those users, as defined below, should not engage in these activities in UTC or outside UTC when using UTC equipment or systems. The UTC policy restricts certain internet usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	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					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 Radicalisation or extremism in relation to the Counter Terrorism and Security Act 2015					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	Threatening behaviour, including promotion of physical violence or mental harm				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	
Using UTC systems to run a private business					X	
Using systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by the UTC / academy					X	
Infringing copyright					X	

Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Creating or propagating computer viruses or other harmful files				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)		X			
On-line gaming (non-educational)		X			
On-line gambling				X	
On-line shopping / commerce		X			
File sharing		X			
Use of social media		X			
Use of messaging apps		X			
Use of video broadcasting e.g. YouTube		X			

Responding to incidents of misuse

It is hoped that all members of the UTC community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

If any apparent or actual misuse appears to involve illegal activity e.g.

- child sexual abuse images
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material, radicalisation and extremism
- other criminal conduct, activity or materials

The SSCB flow chart should be consulted and actions followed in line with the flow chart.

If members of staff suspect that misuse might have taken place, but that the misuse is not illegal it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation

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:

Students / Students **Actions / Sanctions**

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

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

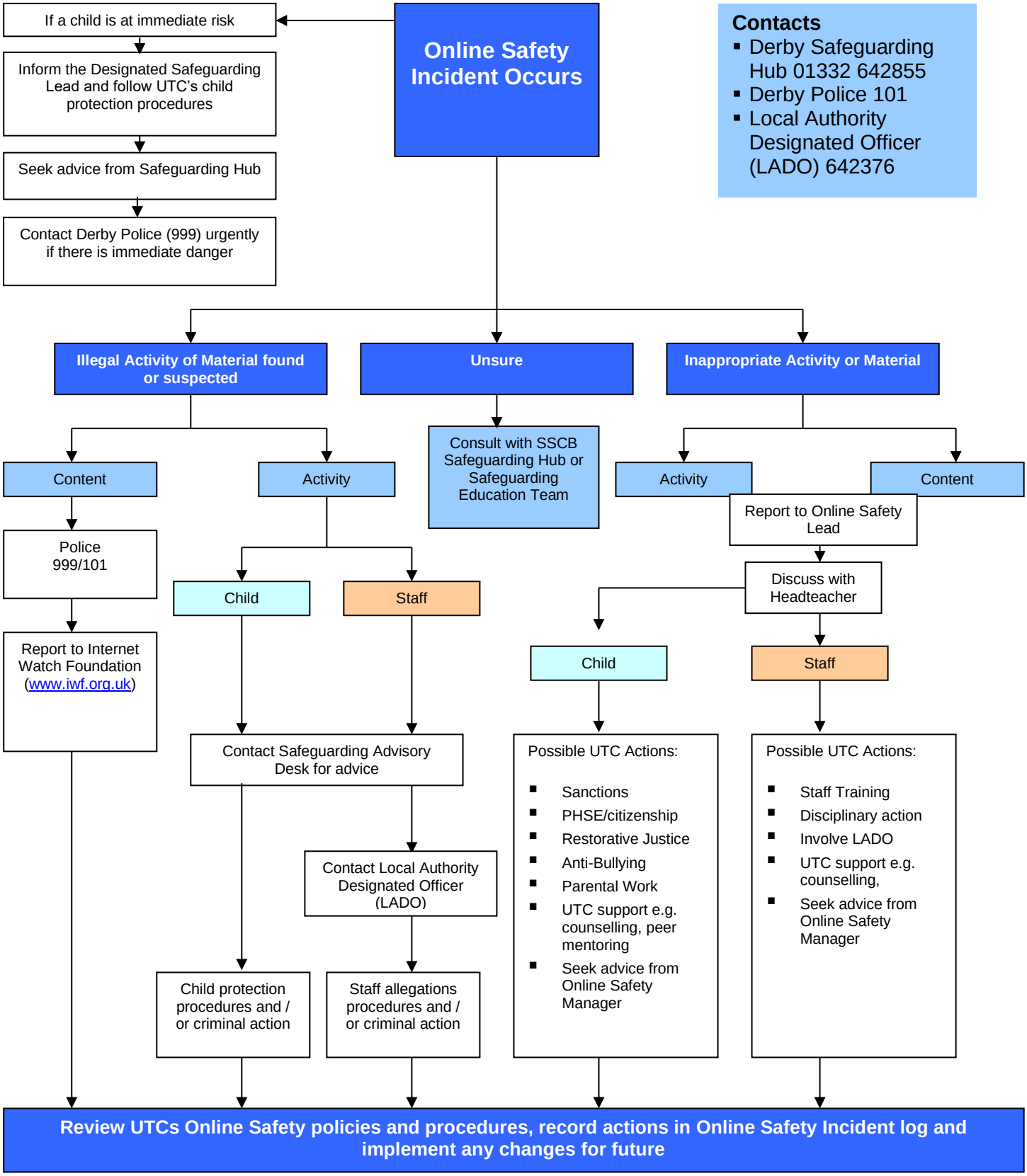
Dealing with Online Complaints

The nature of the internet, and the two-way communication that it brings, means that many parents will now turn to the online world to air their concerns or grievances. UTCs often find that a seemingly minor incident can escalate quite quickly with Facebook pages or groups being formed where parents can discuss issues and gather support. It is advised that there should be a procedure for dealing with online complaints, particularly in relation to derogatory comments made in social networks by parents/carers or other members of the UTC community.

Managing the UTC's digital footprint is as crucial as managing a personal one. This is equally important for UTCs that have a social-media presence as well as those with just a website. Staff must understand the importance of not being drawn into discussions or reacting to complaints. It is vital that all staff, governors, students and parents are aware that official complaints channels exist and that the internet is not a recognised option.

- Parents/Carers are reminded through the acceptable use agreement of appropriate complaints channels and procedures.
- The complaint policy/procedure is clearly detailed on the UTC website and within the Complaints policy.
- All staff and governors are aware of how to report any negative online comments about the UTC or members of the UTC community.
- Staff and governors must under no circumstances reply or react to any online discussion about the UTC unless prior permission has been granted by the Principal.

Response to an Incident of Concern



Contact Details

UTC Designated Safeguarding Lead: Sharon Hunt 477 400
UTC Online Safety Co-ordinator: Sharon Hunt 477 400
UTC Derby Pride Park Principal: Lee Kirkwood 477 400

Appendices

- Student Acceptable Usage Policy
- Staff and Volunteers Acceptable Usage Policy
- Parents / Carers Acceptable Usage Policy Agreement
- Use of Digital Images Consent Form

Acronyms Used	**Definition**
SLT	Senior Leadership Team
AUP	Acceptable Use Policy
DSCB	Derby Safeguarding Children's Board
VLAN	Virtual local area network
BYOD	Bring Your Own Device
PPSK	Private Pre-Shared Key (WIFI password)
CEOP	Child Exploitation and Online Protection
SIRO	Senior Information Risk Officer
IAO	Information Asset Owners

Student Acceptable Usage Policy

Status: Statutory

Member of Staff responsible: Principal

Associated Policies and documentation:

- Online Safeguarding Policy
- Data Protection Policy
- Staff Acceptable Usage Policy
- Parent / Carer Acceptable Usage Policy

Implementation Date: September 2020

Last Review Date: September 2023

Next review date: September 2024

Student Acceptable Use Policy Agreement

UTC Derby Pride Park Policy

New technologies have become integral to the lives of children and young people in today's society, both within UTCs and in their lives outside UTC. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can promote discussion, inspire creativity and stimulate awareness of context to encourage effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that UTC ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.

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

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

For my own personal safety:

- I understand that the UTC will monitor my use of the ICT systems, email and other digital communications
- I will not share my username and password with anyone or try to use any other person's username and password
- I will be aware of the need to keep myself safe when I am communicating on-line
- I will not disclose or share personal information about myself or others when on-line
- If I arrange to meet people off-line that I have communicated with on-line, I will do so in a public place and take an adult with me
- I will immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it on-line

I understand that everyone has equal rights to use technology to support our education:

- I understand that the UTC ICT systems are for educational use and that I will not use the systems for personal or recreational use unless I have permission to do so
- I will not use the UTC ICT systems for on-line gaming, internet shopping, file sharing or video broadcasting (e.g. YouTube), unless I have permission of a member of staff to do so
- I will not use the UTC ICT systems for personal financial gain, gambling, political purposes or advertising at any time

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

- I will respect others' work and property and will not access, copy, remove or otherwise alter any other user's files, without the owner's knowledge and permission
- I will not move computer equipment, unplug cables or remove screws or covers from equipment. I will not place bags near computer equipment and I will not consume food or drink in IT rooms or near IT equipment
- 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
- If I am sending messages or emails I will ensure these are written carefully and politely. I am responsible for the messages and emails I send and for contacts made. I will not send anonymous messages
- I will not use UTC systems to send messages that are unprofessional in tone or contain inappropriate content
- I will not take or distribute images of anyone without their permission.

I understand that the UTC has a responsibility to keep the technology secure and safe:

- I will only use my personal devices e.g. mobile phones, in the UTC if I have permission or in the designated areas at set times i.e. canteen at lunch & break time. I understand that, if I do use my own devices in UTC, I will follow the rules set out in this agreement, in the same way as if I was using UTC equipment
- If I misuse a personal device or use outside of set times and designated areas I understand that my device will be confiscated until the end of the UTC day and a detention issued
- 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 programs or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials
- I will immediately report any damage or faults involving equipment or software, however this may have happened
- I will not open any attachments to emails, unless I know and trust the person / organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes; if in doubt I will check with the IT Services department
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings
- I will only use chat and social networking sites with permission and at the times that are allowed i.e. canteen at lunch & break time
- I understand that when my network account is created an Office 365 account will be generated and linked to enable access to cloud services such as Email, OneDrive, Office Online etc. The minimum amount of information required to create an account is sent to the Microsoft servers in compliance with their data protection policy.

I understand how and when I should use personally-owned devices within the UTC

- I understand that mobile phones and personally-owned devices will not be used during lessons without the explicit permission of a member of staff to support learning. They should be switched off or silent during lesson time unless instructed by the teacher and only used during in designated areas at set times i.e. canteen at lunch & break time and not on corridors

- I understand that mobile phones and personally-owned mobile devices brought into the UTC are the responsibility of the device owner. The UTC accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices
- I understand that mobile phones and personal devices are not permitted to be used in certain areas within the UTC site such as changing rooms and toilets
- I will ensure the Bluetooth function of a mobile phone is switched off at all times and not be used to send images or files to other mobile phones
- I understand that no images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned
- I understand that phones and devices **must not be** taken into examinations. If I am found in possession of a mobile phone during an exam I will be reported to the appropriate examining body. This may result in my withdrawal from either that examination or all examinations
- If I need to contact my parent or carer, then I must report to the Learning Managers or Reception where I will be allowed to use a UTC phone. In some circumstances I will able to use my own phone in the presence of a member of staff
    - Note: Parents are strongly advised not to contact students via their mobile phone during the UTC day, but to contact the UTC Reception:
        - UTC Derby Pride Park 01332 477 400
- I will protect my phone number by only giving it to trusted friends and family members. I will engage with the instruction outlined through my education on the safe and appropriate use of mobile phones and personal devices I will listen to and understand the associated boundaries and consequences.

When using the internet for research for my UTC work, I understand that:

- I should ensure that I have permission to use the original work of others in my own work with the appropriate citation
- 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 find is accurate, as I understand that the work of others may not be correct
- I understand that the UTC will monitor my use of the internet
- I will not make any attempt to bypass the filtering settings provided in UTC.

I understand that I am responsible for my actions, both in and out of the UTC:

- I understand that the UTC could take action against me if I am involved in incidents or inappropriate behaviour that are included in this agreement, when I am out of the UTC as well as in the UTC. Examples of this are online bullying, sending/receiving inappropriate images and misuse of personal information
- I understand that if I do not follow this Acceptable Use Policy Agreement, it will lead to disciplinary action. This may include loss of access to the UTC network / internet, detentions, isolation (Consequences), exclusion, contact with parents and in the event of illegal activities, involvement of the police

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

Student Acceptable Use Agreement Form

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

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

- I use the UTC ICT systems and equipment (both in and out of UTC)
- I use my own equipment in UTC (when allowed) e.g. mobile phones,
- I use my own equipment out of UTC in a way that is related to me being a member of this UTC e.g. communicating with other members of the UTC e.g. through social networks, mobile phones, accessing UTC email, Learning Platform, website etc.

Name of Student:			
Year group:		Tutor group:	
Signed:		Date:	

Derby and Derbyshire
Safeguarding Children Partnership

Staff Acceptable Usage Policy

Status: Statutory

Member of Staff responsible: Principal

Associated Policies and documentation:

- Data Protection Policy
- Online Safeguarding Policy
- Student Acceptable Usage Policy
- Parent / Carer Acceptable Usage Policy

Implementation Date: September 2020

Last Review Date: September 2023

Next review date: September 2024

Staff ICT Acceptable Usage Policy

As a professional organisation with responsibility for children's safeguarding, it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the UTC's computer system in a professional, lawful and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the UTC systems, they are asked to read and sign this **Acceptable Use Policy**.

Private Work:

- UTC Derby Pride Park facilities may not be used, under any circumstances, in the pursuit of commercial or private work. Facilities include equipment used for the creation, storage and transmission of information in electronic form.

Personal Use:

- It is permissible to use such facilities for incidental personal purposes
- This does not include uses requiring significant expenditures of time or uses that would otherwise violate UTC Derby Pride Park policy
- The facilities should be used for personal purposes during lunch times or outside normal working hours
- If staff are examiners for Awarding Organisations they may use UTC equipment to undertake this task, but this **must not** require additional software to be installed and **should not** be undertaken during normal working hours
- No programs or applications for personal use, including games and screen savers, may be copied on to a UTC Derby Pride Park computer
- It is policy not to store any type of commercial music or video on the UTC Derby Pride Park computer systems. Only UTC owned material can be stored.

Email usage:

- Staff have a responsibility to draft all emails carefully, taking into account discrimination, harassment and defamation issues. E-mails should be written carefully, professionally and politely. Users are responsible for the e-mail they send and for contacts made. The sending of anonymous messages, jokes and chain letters is not allowed
- If you send an email to someone by mistake you must report this immediately in accordance with the Data Protection Policy
- E-mails have the same standing in law as signed letters and their content has, therefore, the same force in contractual arrangements
- Staff cannot expect any email messages composed, received or sent on the UTC network to be for private viewing only
- If an e-mail is received with an attachment it **must not** be opened unless it is known who has sent it, if in doubt check with the IT Services Department. Attachments to e-mails are a major source of viruses. Do not open attachments from an unknown sender or where the message is cryptic
- Any misuse of the internet or e-mail systems may result in disciplinary action and the removal of access rights

- Always follow these general e-mail safety rules:
  - Do not to click on suspicious links in e-mail
  - Do not open suspicious e-mail attachments
  - Do not trust an e-mail because it “appears” to come from someone you know
  - If you are not expecting an e-mail of this type/subject be very cautious before opening
  - Make sure you trust the links you are clicking on when searching Google, Bing etc.
  - **ASK IT SUPPORT IF YOU ARE UNSURE!**

Internet usage:

- Staff may access the Internet for their own personal purposes during lunch times or out of normal working hours
- Staff are expected to behave in a responsible manner and not access sites concerned with ‘hacking’, gambling etc.
- The viewing or downloading of racist, homophobic or sexually explicit material, at any time, is a serious disciplinary offence
- Internet use must be appropriate to education
- Copyright and intellectual property rights must be respected
- The use of chat rooms is not allowed
- Use for personal financial gain, gambling, political purposes or advertising is not permitted
- Possession of certain types of unsuitable material may lead to prosecution by the relevant authorities and/or disciplinary action by UTC Derby Pride Park. Any staff member viewing or downloading obscene material would face serious consequences, including disciplinary action
- Staff must not download/store material, such as music/video files, which does not comply with copyright legislation, as this places the UTC at risk of prosecution
- Staff must not download computer programs, as this places the network at risk of virus infection and may breach licensing agreements
- The download of very large files may significantly degrade the performance of the UTC Derby Pride Park network and/or Internet services and so adversely affect teaching and learning. Staff are required to comply with requests to desist from any personal activity which degrades network performance
- The automated filtering systems used by UTC Derby Pride Park are aware of more than one billion unsuitable URL’s, however, no automated filtering system can be completely effective on its own and a combination of approaches is needed. It is acknowledged that adequate supervision is essential, especially when minors are using the Internet. Students should not be left unsupervised whilst using the internet.

Social networking:

- Staff use of social networking sites such as Facebook, Instagram, Twitter etc. must not encompass student followers and staff should not have students or their family members as members, friends or contacts. If members of staff are friends with families prior to their son / daughter commencing their studies at the UTC, this should be declared to SLT
- Communication with students should be through the UTC Derby Pride Park systems only
- It is important to seek advice when using any educational social medium for the purposes of learning with students before you commence

- Your own social networking details should be kept confidential. Privacy controls should be used to limit your 'public profile' to friends and colleagues this information must not be shared or be visible to students.

Monitoring of Use:

- The UTC may engage, for valid business reasons including staff supervision, in the monitoring of all electronic mail messages or other electronic files created by staff. This includes those created for personal use.

Bring Your Own Device (BYOD):

- The use of your own devices to connect to the UTC Derby Pride Park network is entirely at your own risk. Whilst we support the use of personal devices within the UTC we cannot guarantee that they will function reliably
- The usage of personal devices must comply with the UTC's computer usage policies. Photographs, videos or data of any student or group of students should not be stored or accessed via your own personal device. Whilst access to the internet is filtered via the UTC Derby Pride Park network, it is important to note that personal devices such as phones and tablets may have 3G, 4G or 5G connections
- Staff should not use personal devices to bypass UTC Derby Pride Park internet filters. Staff do so at their own risk and any content viewed or accessed this way, where students are present, may lead to disciplinary action.

Laptop Usage Policy:

- The laptop remains the property of UTC Derby Pride Park
- The laptop is to be used for work purposes only
- The laptop is not to be used by any student, staff laptops contain sensitive data
- If the laptop is stolen or sustains damage whilst in your home this will not be covered by UTC Derby's insurance and you will be required to reimburse the UTC (you may be able to claim on your home contents insurance).
- The laptop must not be left in an unattended vehicle and it must be locked in a desk / cupboard (not able to be seen) if left on UTC premises outside of UTC hours
- If the laptop is stolen or damaged under circumstances where the cost cannot be recovered by any insurance you will be expected to reimburse UTC Derby Pride Park
- If your laptop is lost or stolen you must report this immediately in accordance with the Data Protection Policy
- It is your responsibility to keep the laptop in good condition whilst in your care
- You must always save your work to the 'My Documents' folder or the relevant staff work area. If you have problems saving you must report this to the technicians as soon as possible. Personal photographs, music, etc. must not be saved in your personal user area P:\ or 'My Documents', as they will then be copied to the UTC network during synchronisation and take up valuable storage space. If you save personal files to the computer drive this will be at your own risk
- At times it will be necessary to collect laptops in for essential maintenance and upgrades
    - When this takes place we will take the necessary steps to save users work from the user's personal folder P:\ or 'My Documents' folders only. If you have saved outside of these areas, including the G: drive, it is your responsibility to make sure it is backed up elsewhere

- The UTC cannot be held responsible for loss of files that have not been saved in the correct area, including personal photographs and music
    - You must connect to the UTC network at least once per half term in order to pick up anti-virus updates and to synchronise your work, which will then be backed up. Please note that we recommend you connect as often as possible to the UTC Derby Pride Park network
    - You must not install any software without the prior approval of the Network Manager and/or the UTC Senior Leadership Team. You can install printers and other peripheral devices. However, if these devices require drivers you will need to book your laptop in to have the relevant driver installed
    - You can use the laptop for connecting to the internet at home.

Removable media:

- UTC Derby Pride Park has taken the decision that removable media will not be allowed. This includes, but not limited, to USB Flash drives, external hard drives, memory cards, recordable CDs/DVDs etc. If you have been using these devices you must make sure that any UTC Derby Pride Park related information and personal identifiable information is completely deleted from those devices
- As an alternative to removable media, UTC Derby Pride Park offers OneDrive for Business that is part of our Office 365 subscription.

Cloud services & storage:

- Staff must not sync or upload any data from UTC Derby Pride Park to any cloud service except for The Office 365 tenant that belongs to UTC Pride Park (utcderby.org.uk)
- If you access any Office 365 Application or service via a mobile device, you must have 2-factor authentication enabled on your account. Please contact IT Support to enable 2-factor authentication on your Office 365 account
- If you believe you have anything belonging to the UTC on a third party service this must be removed immediately
- Any files containing personal identifiable information that are synchronised or uploaded to any third party service must be reported immediately in accordance with the Data Protection Policy, even if it is removed
- The OneDrive for Business Client must not be installed on any personal device that does not have the same level of security as a UTC Derby Pride Park owned device. This includes a strong password and disk encryption. You can still access files via the web client that does not synchronise anything to the machine
- When a staff network account is created an Office 365 account will be generated and linked to enable access to cloud services such as Email, OneDrive, Office Online etc. The minimum amount of information required to create an account is sent to the Microsoft servers in compliance with their data protection policy.

Passwords:

- The UTC Derby Pride Park network enforces a password policy that requires a minimum password length of 8 characters with a mix of Upper/Lower/Numerical characters
- Passwords are required to be changed every 90 days and the same password cannot be used again
- Passwords are there for security purposes and therefore:
    - Staff must use their own password and never anyone else's

- Staff must never tell anyone their password
- Passwords must not be written down and/or left anywhere that is not secured. They must not be stuck to your monitor or under your keyboard, this would constitute a major security & policy breach. If you need to save passwords we recommend using a reputable password manager. IT Support can help with recommendations with this
- Never use the same password on different systems, always use a unique password
- Think about the password you use. If it is a simple word with a number tagged on the end a malicious system would guess this in a few seconds with todays computing power.

Data Retention:

- Office 365 data, Email inbox, OneDrive files etc. are retained for 30 days after account is marked for deletion
- File Server storage is retained for **no more than one full term** on the file server and then no more than 30 days in backups after data has been removed from the server
- Internet history & Smoothwall logs are kept for 30 days after account deletion
- Printing Information (no more than 1 full term after account deletion).

Further Information

- The UK Safer Internet Centre's Professional Online Safety Helpline offers advice and guidance around Online Safety for professionals who work with children and young people in the UK. The helpline provides support with all aspects of digital and online issues such as social networking sites, cyber-bullying, sexting, online gaming and child protection online. Staff can contact the helpline via 0844 381 4772, helpline@saferinternet.org.uk or can visit www.saferinternet.org.uk/helpline for more information
- "Safer Use of New Technology" is a Kent Safeguarding Children Board (KSCB) document which discusses ideas and FAQs for professionals on how to use technology safely when working with young people. The document can be downloaded from www.kenttrustweb.org.uk?esafety

Staff ICT Acceptable Usage Policy Agreement

The UTC may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the UTC's Data Protection Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the UTC will invoke its disciplinary procedure. If the UTC suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

Equipment Issue

	Asset	**Model**	**Service Tag**	**Machine Name**	**Initial**
Returning					
Issue					

I have read and understood the Staff ICT Acceptable Use Policy:

Name:	**Signed:**	**Date:**
Staff		
IT Support		

Parent / Carer Acceptable Usage Policy

Status: Statutory

Member of Staff responsible: Principal

Associated Policies and documentation:

- Online Safeguarding Policy
- Data Protection Policy
- Student Acceptable Usage Policy
- Staff Acceptable Usage Policy

Implementation Date: September 2020

Last Review Date: September 2023

Next review date: September 2024

Parent / Carer Acceptable Use Policy Agreement

UTC Policy

New technologies have become integral to the lives of children and young people in today's society, both within the UTC and in their lives outside the UTC. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can promote discussion, inspire creativity and stimulate awareness of context to encourage effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use
- that UTC ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk
- that parents and carers are aware of the importance of Online Safety and are involved in the education and guidance of young people with regard to their on-line behaviour.

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

A copy of the Student Acceptable Use Policy is attached to this permission form, so that parents / carers will be aware of the UTC expectations of the young people in their care.

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

Permission Form

Name of Parent / Carer:			
Name of Student:			
Year group:		Tutor group:	
Signed:		Date:	

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

I acknowledge that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, Online Safety education to help them understand the importance of safe use of ICT – both in and out of the UTC.

I understand that the UTC will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I

also understand that the UTC cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the UTC will contact me if they have concerns about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will promote positive, safe and responsible behaviour on the internet. I will inform the UTC if I have concerns over my child's Online Safety.

Signed:		Date:	

Derby and Derbyshire
Safeguarding Children Partnership

Parental Consent Form

Please complete and return to admin reception at UTC Derby with the data collection form. If we need more specific consent we will ask for the individual occurrence.

Child's Name: _____ **Year Gp:** _____

Please indicate your consent by placing a tick in the Yes or No box

	Yes	No
*Photographs displayed in UTC		
*Photographs used in UTC publicity material eg website, media publications, prospectus		
*Photographs used in material by the Baker Dearing Trust		
Sex Education		
UTC trips within local area		

* **Images will only be used on new materials for up to three years but older images may be used for longer**

Do you give your consent to let your child leave the UTC due to Early Closure without contacting you for permission? E.g. bad weather/exceptional circumstances (please tick one box only)

In the event of the UTC needing to close early due to bad weather or other exceptional circumstances what contact do you require?
[Please select one option only]

	Yes	Initial or Signature
I consent to allow the student to leave without contacting parent for permission		
I consent to allow the student to leave without contacting parent for permission but only together with their sibling/s		
The UTC must contact parent or other Emergency Contact for permission for student to leave		

This consent form will remain in place whilst your child is at the UTC – if you or your child wishes to withdraw consent at any time please contact derbyadmin@utcderby.org.uk

Signed by parent …… Date ……

Signed by student …… Date ……