# West Midlands UTC

## E-Safety Policy

| | | | |
|---|---|---|---|
| Author | SMA | Version | 1.1 |
| Governor Approved Date | 10/04/2017 | Last Review Date | 19.02.2018 |
| Comments | This is a statutory policy outlining the structure and arrangements of the WMUTC e-Safety Strategy. | | |
| Monitoring, Evaluation and Review | The Governors will review this document at least once every two years and assess its implementation and effectiveness in consultation with key stakeholders.<br>The Principal retains responsibility for ensuring that the commitments made within this policy are upheld by the UTC. The Vice Principal will monitor and evaluate the impact of the policy and conduct regular consultation with parents, students and staff to ensure that the policy is fit for purpose and being applied consistently. | | |

**Contents**

**Equality and Diversity Statement**

WMUTC strives to treat all its members and visitors fairly and aims to eliminate unjustifiable discrimination on the grounds of gender, race, nationality, ethnic or national origin, political beliefs or practices, disability, marital status, family circumstances, sexual orientation, spent criminal convictions, age or any other inappropriate grounds.

## 1. Introduction

**1.1.** At WMUTC we encourage student engagement with Information and Communication Technology (ICT) as we believe that it enables them to learn, communicate and explore the world in new ways. Many young people are now skilled in using computers, games consoles, mobile phones and tablet computers. However with this new technology we also acknowledge that there are also new risks.

**1.2.** We believe that everyone in our school community is responsible for the welfare and safety of children and it is therefore crucial that all stakeholders understand what these risks are and how we can all work together to enjoy these new technologies safely.

**1.3.** E-Safety is essentially about creating a safe environment when using ICT. This includes the use of the internet and social networking sites. This document is intended to outline the school's approach to preventing safeguarding issues, including cyber bullying, as well as detailing how we respond to e-safety issues when they emerge.

**1.4.** "As in any other area of life, children and young people are vulnerable and may expose themselves to danger - knowingly or unknowingly - when using the internet and other digital technologies. Indeed, some young people may find themselves involved in activities which are inappropriate or possibly illegal." Becta ICT Advice – Safeguarding Children in a Digital World.

**1.5.** Our aim is to address these potential issues by regularly providing clear guidelines and information to students, their parents and staff about how to keep young people safe and by dealing rapidly with any emerging concerns through a consistent approach, as outlined in this document; this will invariably involve close communication with parents and where necessary, liaison with Children's Services, the Police and other relevant agencies.

**1.6.** One of the key risks of using the internet, email or instant messaging services is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all but unfortunately this also means that for example, those with extreme political, racist, sexual or other prejudiced views are able to publicise those opinions.

**1.7.** In the case of pornography and indecent images of children, there is no doubt that the internet plays host to a large amount of legal and illegal material. Curiosity about pornography is a normal part of sexual development but young people may be shocked by some of the material online and it is not known what the long-term effects of exposure to such images may be.

Seeking out some aspects of pornography is a criminal offence and could result in a criminal conviction.

**1.8.** The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the internet and other technologies and is probably the risk most reported by the media. A criminal minority make use of the internet and related services such as chat rooms to make contact with young people. The intention of these individuals is to establish and develop relationships with young people with the sole purpose of persuading them into relationships which can then progress to sexual activity. Child sex offenders will often target specific individuals, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. Such behaviour is known as 'grooming'.

## 2. Roles and Responsibilities

**2.1.** As a school we see it as our responsibility to respond to e-safety concerns, irrespective of whether they occur inside or outside of school. Breaches to our school network protocols will be dealt with rapidly by SLT in liaison, where appropriate, with the DSL and/or other relevant pastoral leaders. However, where the school receives information of a safeguarding nature concerning online activity which has taken place outside school, the school is equally committed to engaging with the students concerned and their parents to resolve the situation. Where we feel there is an ongoing risk to a young person, Children's Services and occasionally the Police, may be contacted to provide further support.

**2.2.** It is the responsibility of all members of our school community, including teaching and non-teaching staff, governors, volunteers and students, to prevent and tackle e-safety issues. In line with the school's Safeguarding Policy, all e-safety concerns should be shared at the earliest opportunity with the DSL (Simon Maxfield) or Deputy DSL (Tom Macdonald, Claire Gleeson or Simon Smith) and in any case before the end of the school day. The DSL is responsible for ensuring that technical staff are aware of what constitutes an e-safety concern which it would be necessary to report. The DSL will report regularly to the safeguarding governor on incidents of e-safety concerns and the subsequent actions and outcomes within the school.

**2.3.** The Principal is responsible for ensuring that e-safety concerns are monitored and that staff remain appropriately trained to respond to such concerns. It is also the responsibility of the Principal to ensure that preventative work is ongoing with students and that awareness raising among parents is ongoing.

## 3. Recognition and Response

**3.1.** All members of our school community should be alert to the possibility that:

**3.1.1.** A child may already have been/be being abused and the images may have been distributed on the internet or by mobile telephone;

**3.1.2.** An adult or older child may be grooming a child for sexual abuse, including for involvement in making abusive images. This process can involve the child being shown abusive images;

**3.1.3.** An adult or older child may be viewing and downloading child sexual abuse images.

## 4. Concern about Student Safety or Adult Behaviour

**4.1.** Any member of staff who has a concern about any safeguarding issue should complete a safeguarding referral form (available in workrooms, general office and attached to the safeguarding policy) and inform the Designated Safeguarding Lead (DSL) or one of the Deputy DSLs as a matter of urgency and before the end of the school day. A concern should be shared even where there is no evidence to support it.

**4.2.** The DSL/Deputy DSL should follow the procedure set out in the school's Safeguarding Policy to assess whether a referral should be made to Children's Services.

**4.3.** If a decision is made not to refer to Children's Services, the school will still keep a record of the concerns in the student's Safeguarding file for reference should further concerns emerge at a later date.

**4.4.** Where specific children are identified as abused in the production of indecent images of children, a Section 47 Enquiry should be carried out by Children's Services and WMUTC will work closely with Children's Services, fully sharing information, to support the students throughout this time.

**4.5.** It is important to be aware that the child may not want to acknowledge his/her involvement in such behaviour or admit their abusive nature and may resist efforts to be offered protection. This should not be a deterrent and WMUTC will work closely with other agencies in order to continue to monitor and assess the nature and degree of any risk to the child.

**4.6.** Where there is concern about an adult, but there is no identifiable child, a referral will be made to the Police and to Children's Services, enabling them to initiate an investigation.

## 5. Allegations Against People Who Work With Children

**5.1.** All members of our school community should be aware of their responsibility to follow safeguarding procedures if they have a concern that adult staff members or volunteers may be accessing indecent images of children. Employees of the school are regularly made aware of the Whistleblowing Policy and the Principal must follow Wolverhampton Safeguarding Children's Board interagency procedures in dealing with such allegations. The Local Authority Designated Officer (Paul Cooper) holds the responsibility for ensuring that allegations against members of staff are properly investigated. WMUTC follows the guidance of the local authority and WSCB procedures in all cases where it is alleged that a person who works with children has:

**5.1.1.** behaved in a way that has harmed a child, or may have harmed a child;

**5.1.2.** possibly committed a criminal offence against or in relation to a child;

**5.1.3.** behaved toward a child or children in a way that indicates she or he is unsuitable to work with children.

**5.2.** In operating the WSCB procedures the school must consider whether the allegation can be properly investigated if the person concerned remains in work. Schools can seek advice about suspension and alternatives to suspension but the final decision remains with the school. It would be very unusual for the school not to take the advice of WSCB and if it were to do so, WSCB may decide to take the issue to the education secretary.

**5.3.** It is important that individuals suspected of accessing, creating or downloading indecent images of children are not alerted prior to the police undertaking their investigations as they may destroy computer evidence at work or home. This has implications for managing allegations against people who work with children and means individuals may not initially be fully informed of reasons for their suspension.

**5.4.** Research into investigations of adults accessing child abuse images has identified that professional staff accessing such images may have access to children both in their occupation and in their personal lives. In such cases, a section 47 strategy discussion (Children Act 1989) will consider the need to assess risk both in relation to the occupation and in relation to the risk to any child within the family of the individual concerned. The Principal and/or the DSL will be involved in this strategy meeting.

## 6. The Risks Posed By New Technology

**6.1.** As with many new or and emerging technologies, the internet has brought unfamiliar challenges, some of which create actual or potential dangers for children and young people. New technologies have offered children and young people revolutionary advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. The main risks are in relation to sexual exploitation and the use of technology to bully and record physical abuse.

**6.2.** Some of the most common risks to children and young people are as follows:

**6.2.1. Children viewing adult pornography**

**6.2.1.1.** Children & young people often access adult pornography. However, the persistent viewing of material which is degrading, violent or sadistic or beyond the realms of normal curiosity can affect how young people can think about intimacy, themselves and their values and attitudes towards relationships and sexual development. Adult pornography can also be used by adults or young people as part of a grooming process.

**6.2.2. Children abused through using the Internet and mobile phones**

**6.2.2.1.** New technologies such as chat rooms and SMS are often used by those wanting to sexually exploit children and young people. These perpetrators often exploit young people who are vulnerable by grooming them.

**6.2.2.2.** Children can be coerced to take part in sexual activity online by abusers who employ specific conversational techniques. The grooming process is no different from that used by abusers offline. However, the whole abusive episode takes place online without physical contact between the child and perpetrator. The most common place for targeting these children is in social networking sites and chat rooms. When discovered, children will often deny any such activities, due to both the grooming process and the shame that many children feel when discovered doing something that have been told not to reveal and about which they feel deep humiliation and fear.

**6.2.3. Young people creating and sending indecent images of themselves to others**

**6.2.3.1.** Occasionally young people choose, or are coerced, into creating and sending indecent images of themselves to others. This can sometimes be vulnerable individuals who have been made to feel special and have been convinced that the other person involved loves them or is attracted to them. Often the other individual might promise to delete the images or to keep them secret. This can lead to considerable distress for the victim if the abuser then choses to publicise the images. It can also result in blackmail if the victim says no to creating and sending further, more explicit images.

**6.2.4. Children, who create, view or download sexually abusive images of other children**

**6.2.4.1.** Although some children plan to and purposefully download these images, others may have been forced to do so by peer group pressure or they may have been introduced to these sites by predatory adults as part of grooming for sexual abuse.

**6.2.5. Young people creating or placing images of other young people online**

**6.2.5.1.** The use of the internet as a tool for bullying is also becoming increasingly common. 'Happy slapping' and other recorded physical assaults, for example, can be carried out with the intention of humiliating, compromising or exploiting the young person who is the subject of the image.

**6.3. Children groomed online for sexual abuse offline**

**6.3.1.** It is an offence to groom a child. Sometimes children are befriended online by individuals with the sole purpose of gaining their trust. Often they may lie about their age and background to appeal to the young person, building up their trust until a point when they can suggest that they meet. While this is rare, research shows that in the UK, over eight million children have access to the internet and a significant proportion of these children (one in twelve) have met in person with someone who they first met online.

**6.4. Children made the subject of child abuse images or pseudo-images**

**6.4.1.** Children who are the subject of child abuse images may suffer incalculable trauma which may affect them for the rest of their lives. Perpetrators often use strategies to inhibit children disclosing the abuse: children may be shown abusive images of other children or their own abusive images in an attempt to normalise the activity; abusers may encourage children to place images of themselves or friends online;

victims may be encouraged to be proactive in either their own sexual abuse or that of other children.

**6.4.2.** Pseudo images may be created of particular children by the technological manipulation of existing photographs, art or cartoons. These images often have the same impact on the victim as non-pseudo images.

## 7. Our response to e-safety risks to students

**7.1.** In all cases of e-safety concern, WMUTC follows the school's Safeguarding Policy to ensure concerns are reported appropriately as a matter of urgency and on the same day of a concern emerging, to the DSL or the DDSL. Where a risk is deemed to exist, parents, Children's Services and where appropriate, the Police will be informed. An assessment will usually be carried out by Children's Services to ensure that victims are fully protected and that the behaviour of child perpetrators is fully addressed.

**7.2.** Where it is felt that an ongoing risk is not a concern, the school is likely, usually following advice from Children's Services, to deal with the issues directly with students and their parents. This may involve meetings with students and parents whereby boundaries/ restrictions to internet access may be imposed. The school may choose to involve external agencies such as the Police or the Sexually Inappropriate Behaviour Service (SIBS) as a way of educating young people further about risk, online safety. For child perpetrators, this may involve work which focuses on respecting themselves and others. Additionally, short courses run by our school counsellor or our school Student Welfare Leader may be used to educate, with the intention of altering perceptions and behaviour.

**7.3.** Education is the key to minimising the online risks to students. Self & Society sessions and Assemblies throughout the year are used regularly to educate students on appropriate online behaviour. These sessions address the school's moral and ethical stance, provide information for victims and their families and friends of where to go and what will happen next, as well as outlining the consequences for perpetrators.

**7.3.1.** These sessions address the following:

**7.3.1.1.** our approach to cyber bullying, with specific reference to our Anti Bullying Policy;

**7.3.1.2.** the safe use of social media, including utilising privacy settings and the pitfalls of sharing personal information and photographs;

**7.3.1.3.** the significance and consequences of their online behaviour, including digital footprints, legal sanctions and career prospects;

**7.3.1.4.** online stranger danger, including how to recognise and report suspicious activity;

**7.3.1.5.** the school's response to online behaviour that may bring the school or its members into disrepute.

**7.3.1.6.** awareness of the dangers of 'live streaming' via current apps and social media sites in relation to cyber bullying and youth produced sexual imagery.

**7.3.2.** The Child Exploitation and Online Protection Centre (CEOP, http://www.ceop.police.uk/) brings together law enforcement officers and specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. CEOP's 'Report Abuse' button is on the home page of our school's website and every year students are informed of how to use this facility to report online abuse.

**7.3.3.** Annual training for all staff and new staff induction sessions, highlight the school's Social Networking Policy which informs all staff of our expectations in terms of protecting their identity and upholding an online presence that is appropriate to their professional position. All staff are made aware that it is a breach of our Social Networking Policy to have students as 'friends' on social media and that students and staff members should not communicate via personal telephone or email accounts. Staff are also made aware that their online posts which may bring the school into disrepute are not acceptable under the Social Networking Policy.

**7.3.4.** Online training for parents and carers address e-safety issues associated with social media and online communities. These articles outline the measures parents can take to educate and protect their children at home as well as informing them of the school's approach in terms of prevention and response to concerns.

## 8. Cyber-Bullying

**8.1.** Bullying may be defined as deliberately hurtful behaviour, usually repeated over a period of time, where it is difficult for those bullied to defend themselves. In school we use the definition 'Several Times on Purpose (STOP)', It can take many forms but the main types are:

**8.1.1.** physical (e.g. hitting, kicking, theft)

**8.1.2.** verbal (e.g. racist or homophobic remarks, threats, name-calling)

**8.1.3.** emotional (e.g. isolating an individual from the activities and social acceptance of their peer group)

**8.2.** "The damage inflicted by bullying (including cyberbullying via the internet) can frequently be underestimated. It can cause considerable distress to children, to the extent that it affects their health and development or, at the extreme, causes them significant harm (including self-harm). All settings in which children are provided with services or are living away from home should have in place rigorously enforced anti-bullying strategies." (Paragraph 11.57, Working Together 2010).

**8.3.** New technologies have offered children and young people innovative advances in communication with their peers and with the world. However, they also afford an opportunity for misuse and abuse. Bullying through technology (cyber-bullying) can be devastating for the victim and unlike in the real world, the victim can be targeted at any time day or night, home or school.

**8.4.** Bullying can include emotional and/or physical harm to such a degree that it constitutes significant harm.

**8.5.** All staff at WMUTC are aware of the need to be alert to cyber bullying and in line with our Conduct and Anti Bullying Policy, staff are expected to report all instances of bullying, including racist and homophobic bullying, to the Student Welfare Leader or SLT, who will address these issues as a matter of urgency.

**8.6.** More serious cases of bullying or ongoing bullying following intervention should be discussed with the school's DSL/DDSL and could involve making a referral to Children's Services. Separate referrals for assessment and support may be made in respect of both child victim and child abuser.

**8.7.** The DSL and other staff are trained in recognising the differences between bullying and peer on peer abuse. The DSL will be involved in all reports of bullying / peer on peer abuse to quality assure the judgements being determined by staff dealing with the issue.

**8.8.** Where the bullying involves an allegation of crime (threats of assault, theft, harassment) a referral may be made to the police.

**8.9.** Information about good practice in anti-bullying strategies (real & virtual) for schools, can be accessed at;

**8.9.1.** https://www.education.gov.uk/publications/standard/publicationDetail/Page1/DFE-RR098

## 9. Systems and Procedures

**9.1. Infrastructure** – Procedures are in place to protect the school and its students from a malicious cyber-attack. All computer equipment is protected by the security of the school. All external doors to buildings are locked. Visitors to the site are booked in. Servers, PBX and network storage are kept in locked rooms with restricted access. Network communications equipment is kept in locked cabinets. The school network is protected behind a Firewall to protect from external malicious attack.

**9.2.** Access to Servers and Network is limited to a few school technical staff and the selected ICT support company. Individual user ids are used and are protected with strong passwords that change monthly.

**9.3.** Any attempt internally at unauthorised access to servers is logged by the forensic software.

**9.4.** All user data is backed up daily. Critical servers are backed up weekly.

**9.5.** The school uses VLANs to restrict activity and access as appropriate.

**9.6. Downloading software** – In order to prevent unauthorised users downloading software on school devices, laptops and desktop PCs are protected by user names and passwords. Students are automatically blocked from downloading software and virus guards are installed so that staff who download software can do so safely.

**9.7. Passwords and security** – Access to school networks and devices is controlled through careful password procedures, whereby students are required to have passwords of a good strength, before setting strong passwords of six characters which include upper and lower case letters. Additionally, each user has a home folder on the server which cannot be accessed by other users. Students and staff also have access to their own designated shared areas which contain resources.

**9.8.** School IT induction for staff ensures that they are briefed on the dangers of viruses and attachments. Emails are regularly sent out reminding staff of the need to be vigilant.

**9.9. External service providers** – The school is cautious in using external internet services and as such, for third party vendors, it is required that any internet access for students is only provided through the school's internet filter and forensic software.

9.9.1. The school has an e-mentoring solution to provide a monitored and secure communication service with employer mentors.

9.9.2. The school employ the services of 'Forensic Monitoring Solutions'. This company have monitoring clients on all devices and review possible concerns before communicating with the DSL. In low level cases, this communication will be a report sent as a secure email. In more concerning instances, the company will telephone and request a conversation with the DSL directly, in addition to their email. This solution means that well qualified staff are reviewing reports as part of a dedicated service.

**9.10.** **Guest access** – Procedures are in place to provide internet access to temporary staff such as trainee teachers, through temporary user IDs. Guest wifi is also available to allow guest access to the internet but not the local school network. This is provided through a 'ticketing system'.

**9.11.** **Internet filtering** – The school uses 'LightSpeed', a Firewall hardware package, to filter internet content. This is run on a proxy in school. All internet traffic goes out through the school LightSpeed so is filtered and monitored.

9.11.1. Forensic Monitoring Solutions software provides a forensic logging ability and inappropriate use or attempt is logged. These logs are actively monitored. The logging also applies to staff but is not actively reviewed.

9.11.2. Students are limited by blocking lists which restrict content. However different levels of blocking can be applied to different year groups. This is done on a request basis, linked to curriculum needs.

9.11.3. Students and staff who attempt to access a blocked site are informed by a LightSpeed screen message. Additionally, the Acceptable Use Agreement includes statements on logging and monitoring of school ICT equipment.

9.11.4. Should a member of staff require the temporary lifting of a website restriction they are required to inform the ICT technician in school and the information is logged.

**9.12.** **Monitoring digital platforms** - user logins, user printing, user door access, internet access and inappropriate activity on PCs and laptops are all monitored and reported to the appropriate school leader if concerns arise.

## 10. **Related Documents and Timescales**

**10.1.** This policy should be read in conjunction with the following policies and procedures:

10.1.1. Safeguarding Policy

10.1.2. Student Conduct Policy

10.1.3. Anti-Bullying Policy
10.1.4. Social Networking Policy
10.1.5. Whistleblowing Policy
10.1.6. Acceptable Use Policy –Staff
10.1.7. Acceptable Use Policy – Students

## 11. **Further guidance and support (For Professionals)**

**11.1.** Wolverhampton Safeguarding Children Board; https://www.wolverhamptonsafeguarding.org.uk/

**11.2.** On this inter-agency web-site there is specific web-site information designed to offer support and guidance. https://www.wolverhamptonsafeguarding.org.uk/safeguarding-children-and-young-people/i-work-with-children-young-people-families/bullying-and-e-safety

**11.3.** The UK Council for Child Internet Safety (UCCIS) ukccis brings together over 160 stakeholders from across the internet safety spectrum who have come together to work in collaboration for the good of children and families. http://www.education.gov.uk/

**11.4.** The Child Exploitation and Online Protection Centre (CEOP), brings together law enforcement officers, specialists from children's charities and industry to tackle online child sexual abuse. CEOP provides a dedicated 24 hour online facility for reporting instances of online child sexual abuse. www.ceop.police.uk

**11.5.** Think U Know - a website for professionals (and children, young people and parents) full of information and resources about staying safe online. http://www.thinkuknow.co.uk

**11.6.** Barnardo's "Just One Click" Report – http://www.barnardos.org.uk

**11.7.** The Virtual Global Taskforce (VGT) was created in 2003 as a direct response to lessons learned from investigations into online child abuse around the world. It is an international alliance of law enforcement agencies working together to make the Internet a safer place. www.virtualglobaltaskforce.com

**11.8.** The Internet Watch Foundation - This is an organisation, which works with the Police and Internet Service Providers to trace those responsible for putting harmful or illegal material on the web. It also encourages web surfers who find harmful or illegal material to report it. http://www.iwf.org.uk

**11.9.** The Black Country and Birmingham "Stop it Now!" Campaign. http://www.stopitnow.org.uk

**11.10.** For more information on tackling bullying go to: http://www.education.gov.uk/aboutdfe/advice/f0076899/preventing-and-tackling-bullying/what-is-bullying and http://www.education.gov.uk/schools/pupilsupport/behaviour/bullying

**11.11.** The How 2 Be Safety Centre – Set up by the former head of CEOP to support students and staff in keeping young people safe on the internet. https://h2bsafetycentre.com/

12. **Further Guidance and Support (For Parents and Young People)**

**12.1.** The following information gives advice to parents and children in terms of considering the dangers and managing risks, as well as information about computer software and supervised chat rooms etc.

12.1.1. Think U Know - a website for children, young people, parents and professionals full of information about staying safe online. http://www.thinkuknow.co.uk

**12.2.** Clever Click - Click Clever Click Safe Code has been designed to act as an everyday reminder of simple good behaviours, to help children and their carers to avoid common risks online. http://clickcleverclicksafe.direct.gov.uk/index.html

**12.3.** The How 2 Be Safety Centre – Set up by the former head of CEOP to support students and staff in keeping young people safe on the internet. https://h2bsafetycentre.com/

Appendix A

WEST MIDLANDS **UTC**

## Student & Parent Acceptable Use Agreement

### UTC Policy

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

*This Acceptable Use Agreement is intended to ensure:*

- that young people will be responsible users and stay safe while using the internet and other digital technologies for educational, personal and recreational use.
- that UTC systems and users are protected from accidental or deliberate misuse that could put the security of the systems and will have good access to digital technologies to enhance their learning and will, in return, expect the *students / pupils* to agree to be responsible users.

### Acceptable Use Policy Agreement

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

*For my own personal safety:*

- I understand that the UTC will monitor my use of the systems, devices and digital communications.
- I will keep my username and password safe and secure – I will not share it, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will be aware of "stranger danger", when I am communicating on-line.

- I will not disclose or share personal information about myself or others when on-line (this could include names, addresses, email addresses, telephone numbers, age, gender, educational details, financial details etc )
- 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 as a resource and:*

- I understand that the UTC systems and devices are primarily intended for educational use and that I will not use them for personal or recreational use unless I have permission.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not use the UTC systems or devices for on-line gaming, on-line gambling, internet shopping, file sharing, or video broadcasting (eg YouTube), unless I have permission of a member of staff to do so.

*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 be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will not take or distribute images of anyone without their permission.

*I recognise that the UTC has a responsibility to maintain the security and integrity of the technology it offers me and to ensure the smooth running of the UTC:*

- I will only use my own personal devices (mobile phones / USB devices etc) within the UTC if I have permission. I understand that, if I do use my own devices in the UTC, I will follow the rules set out in this agreement, in the same way as if I was using UTC equipment.
- I understand the risks and will not try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others, nor will I try to use any programmes or software that might allow me

to bypass the filtering / security systems in place to prevent access to such materials.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.
- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person / organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not install or attempt to install or store programmes of any type on any UTC owned device, nor will I try to alter computer settings.
- I will only use social media sites with permission and at the times that are allowed.

*When using the internet for research or recreation, I recognise that:*

- I should ensure that I have permission to use the original work of others in my own work
- Where work is protected by copyright, I will not try to download copies (including music and videos)
- When I am using the internet to find information, I should take care to check that the information that I access is accurate, as I understand that the work of others may not be truthful and may be a deliberate attempt to mislead me.

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

- I understand that the UTC also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of the UTC and where they involve my membership of the UTC community (examples would be cyber-bullying, use of images or personal information).
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the UTC network / internet, detentions, suspensions, 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 systems and devices.**

## Student / Pupil Acceptable Use Agreement Form

This form relates to the ***Student*** Acceptable Use Agreement, to which it is attached. 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 UTC systems.

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

- I use the UTC systems and devices (both in and out of UTC)
- I use my own devices in the UTC (when allowed) e.g. mobile phones, gaming devices USB devices, cameras etc.
- I use my own equipment out of the UTC in a way that is related to me being a member of this UTC eg communicating with other members of the UTC, accessing email, VLE, website etc.

Name of Student: **(BLOCK CAPITALS)** ..........................................................................................

Signed: ..........................................................................................

Date: ..........................................................................................

## *Parent / Carer Countersignature*

Name of Parent: **(BLOCK CAPITALS)** ..........................................................................................

Signed: ..........................................................................................

Date: ..........................................................................................

***For office use***

| | | | |
|---|---|---|---|
| **Username** | | **Date** | |

*For office use*

| | | | |
|---|---|---|---|
| **Username** | | **Date** | |

Appendix B

WEST MIDLANDS **UTC**

## Acceptable Usage Policy

## Staff, support staff, governors, visitors, wider stakeholders with access and external contractors

I will only use the UTC IT systems, external logins and email for UTC related purposes. Other use will be with the permission of a SLT teacher.

I will not divulge any UTC related passwords and I will comply with the UTC IT security procedures.

I will make sure email and social media interactions with staff, parents, pupils and members of the public are responsible and in line with the UTC policies and DfE/GTC/TA guidelines.

I will not give my home address, phone number, mobile number, personal social networking details or email address to pupils. I accept that pupils may find these details out, and that any contact should be logged and either not reciprocated, or replied to in line with the UTC policies. I should be responsible and aware of my professional responsibilities and the UTC policies if I supply any personal details to parents.

I will use the UTC email systems for UTC related communications. I will not use personal accounts for UTC business.

I will ensure that personal data is stored securely and in line with the Data Protection Act. I will follow the UTC policy with regard to external logins, encrypted data and not storing UTC material on personal IT equipment.

I will not install software onto workstations or the network unless supervised by the Network Manager or IT support staff.

I will not search for, view, download, upload or transmit any material which could be considered illegal, offensive, defamatory or copyright infringing.

Photographs of staff, pupils and any other members of the UTC community will not be used outside of the internal UTC IT network unless written permission has been granted by the subject of the photograph or their parent/guardian. I will ask the permission of the Principal (on site) or the proprietor of the building (off site) prior to taking any photographs.

I am aware that all network and Internet activity is logged and monitored and that the logs are available to SLT in the event of allegations of misconduct.

I will not write or upload any defamatory, objectionable, copyright infringing or private material, including images and videos, of pupils, parents or staff on social media or websites in any way which might bring the UTC into disrepute.

I will make sure that my Internet presence does not bring the teaching profession into disrepute and that I behave online in line with DfE, GTC and TA guidelines.

I will champion the UTC's e-safety policy and be a role model for positive and responsible behaviour on the UTC network and the Internet.

**Print Name:_______________________________________________**

**Signed:** ________________________________________________
**Date:**__________________________________