UKTD ICT Acceptable Use Policy		
Issued By: Helen Blackbourn Regional Manager / Lead DSO	**Issue No**: v3	**Date of Issue:** March 2020
Approved by: Senior Management Team / IT Systems & Field Support	**Signature** (hard copy signed)	**Review Date**: March 2021

INTRODUCTION

UKTD recognises the vital role that ICT plays in education and the delivery of teaching and learning. Not only is it an essential resource that supports our everyday business functions, but also creates opportunities for learners to develop their skills, extend their knowledge and understanding, become inspired and interact with the outside world.

UKTD also acknowledges that ICT can present risks as well as benefits, particularly to vulnerable individuals who may be influenced by unsuitable online material. Vast amounts of information is shared and communicated via the internet and social media and this can be exploited to cause harm and create safeguarding, radicalisation/extremism concerns.

A key priority for UKTD is to maximise the educational benefits of ICT whilst minimising potential online risks. This policy sets out the conduct and behaviours expected of UKTD employees and reinforces our commitment to creating a culture of safety.

POLICY STATEMENT

1. UKTD will carry out its responsibilities under current legislation and follow statutory safeguarding and Prevent duty guidance.

2. UKTD will make clear to learners and staff what the expectations are regarding the safe use of ICT and ensure that both staff and learners know how to report a concern.

3. UKTD is committed to creating a culture of safety and aims to protect learners from harm, as far as is reasonably practicable.

4. UKTD recognises that misuse of ICT by staff or learners can occur eg:
   - Accessing offensive or unacceptable material.
   - Accessing extremist or radicalisation content.

5. UKTD will ensure that employer partners, trainers and staff working with learners on employer premises understand their responsibilities under the Prevent duty.

6. UKTD staff and employer partners will be made aware of the importance of being vigilant to any unsuitable material that learners may have access and to report any concerns.

7. UKTD will work with appropriate agencies and in particular Prevent partners to ensure a co-ordinated approach to identifying concerns, sharing information and taking prompt action.

8. UKTD recognises its responsibility in implementing and maintaining systems that block inappropriate sites to ensure that the procedures work to prevent risks of radicalisation or grooming.

SCOPE & PURPOSE

This policy applies to all employed staff, freelance contractors, volunteers, employer partners, workplace staff and trainers, and others who work in or on behalf of UKTD. It also applies to all learners that use and access computers, ICT systems, hardware and software made available by UKTD.

UKTD is committed to and will promote the protection and safeguarding of all children, young people and adults at risk who use our services. The purpose of this policy is to ensure that:

- Staff are clear about their responsibilities for ICT usage, act as role models for learners and give clear guidance to learners on acceptable and safe usage.
- Staff are clear that UKTD's Safeguarding Code of Conduct includes ICT Acceptable Use responsibilities.
- Staff are provided with the knowledge and support to be able to recognise, effectively report and escalate any safeguarding or Prevent ICT concerns to the Designated Safeguarding Lead or local Designated Safeguarding Officer.
- Employers and managers at work placements understand their responsibilities for safeguarding and Prevent and follow the procedures that are set.

This policy aims to:

- Clearly state what is deemed to be acceptable use of UKTD computing and ICT resources and supports UKTD's duty to help Prevent and limit the risks of individuals being drawn into terrorism and /or extremism.
- Establish and maintain an environment where all learners feel secure, are encouraged to talk and are listened to if they have a worry or concern.
- Ensure all learners know that there are staff at UKTD whom they can approach if they have a concern.
- Ensure that all learners are taught about safeguarding, radicalisation and extremism and online safety, and are given opportunities to discuss these topics.
- Emphasise, to both staff and learners, the importance of using ICT technology in a responsible way that ensures both legal compliance and online safety.

RESPONSIBILITIES

Acceptable use of UKTD ICT equipment and systems is everyone's responsibility and all users are responsible for adhering to this policy. UKTD cannot accept responsibility for ensuring all actions of users are acceptable but will take reasonable steps to block inappropriate sites, set standards of acceptable use (as in this policy) and take swift action if unauthorised or inappropriate ICT use is identified or disclosed. In all cases the user(s) concerned will be considered liable for their actions.

Contacts for Reporting Concerns

Safeguarding: Prevent Main Single Point of Contact (SPOC)
Helen Blackbourn, UKTD Lead Designated Safeguarding Officer – 07875 665934

Deputy Single Points of Contact: Debby Cramphorn-Arnold (07875 665781) & Tracey Holden (07392 873584), UKTD Designated Safeguarding Officers

ICT System / Equipment Misuse:
Paul Nugent, UKTD IT Systems & Field Support – 01442 915828

ONLINE SAFETY, SAFEGUARDING & PREVENT

> ***"The use of technology has become a significant component of many safeguarding issues. Child sexual exploitation; radicalisation; sexual predation: technology often provides the platform that facilitates harm."***
> (DfE Keeping Children Safe in Education 2019)

The risks associated with online safety have been categorised into three areas:

1) **content**: being exposed to illegal, inappropriate or harmful material; for example pornography, fake news, racist or radical and extremist views;
2) **contact:** being subjected to harmful online interaction with other users; for example commercial advertising as well as adults posing as children or young adults; and
3) **conduct**: personal online behaviour that increases the likelihood of, or causes, harm; for example making, sending and receiving explicit images, or online bullying.

UKTD are committed to doing all it reasonably can to limit learners' exposure to online risks and have filters and monitoring systems in place. An important aspect of this is to focus on internet security and to educate our staff and learners about online safety.

> ***"The internet is a powerful tool which terrorists exploit to radicalise, groom and recruit vulnerable individuals, and to incite and enable terrorist attacks. Terrorist groups make extensive use of different online platforms to communicate with thousands of individuals, spreading their pernicious ideology and propaganda".*** (CONTEST Strategy 2018)

As part of our Prevent duty and overall safeguarding duty of care, UKTD trains all teaching and support staff to be aware of and, if required, act to reduce the threat to the UK from terrorism, by stopping young or vulnerable people becoming terrorists or supporting terrorism. Our learners are taught about online safety and given opportunities to develop the skills they need to recognise and stay safe from the risks of online abuse or harm. We also work closely with employers to ensure they understand their responsibilities for safeguarding and follow the procedures that are set.

Staff need to be vigilant and report any Prevent duty concerns to the Main Single Point of Contact (SPOC) or in their absence report to a Designated Safeguarding Officer (DSO), in line with UKTD Safeguarding and Prevent Policies. In an emergency situation, contact the Police immediately and ask to speak to a Prevent Officer.

Some possible indicators of observed behaviour that may be a concern:

- Becoming withdrawn or disengaged
- Changes of mood, patterns of behaviour or secrecy
- Becoming upset or outraged after using the internet or texting
- Isolation from friends and/or family
- Possessing or having access to violent or extremist literature
- Expressing extremist language or views
- Displaying a sudden increase in wealth or possessions
- Unexplained absence from work

If a learner experiences any form of cyber-bullying or exposure to harmful online material, this needs to be reported to a Designated Safeguarding Officer immediately so that action can be taken.

UKTD ICT ACCEPTABLE USE POLICY GUIDANCE

UKTD provides employees with access to a range of ICT equipment and systems to enable individual job roles to be carried out.

The aim of this guidance is to:

- support an effective teaching and learning environment for all UKTD IT users;
- ensure that users do not use UKTD IT systems to break the law;
- help safeguard learners from IT-based threats.

1) TERMS OF USE

These guidelines apply to all computers, laptops, mobile devices, software and data belonging to UKTD.

It includes use of the ePortfolio system and covers remote access regardless of which device is used to make the connection e.g. personal computer at home or mobile device. These resources are provided on the understanding that they are not misused in any way that will interfere with, disrupt or prevent anyone from legitimately using UKTD resources.

Use of ICT facilities is subject to the provisions of the following legislation:

- Copyright, Design and Patents Act 1988
- Protection from Harassment Act 1997
- Malicious Communications Act 1988
- Computer Misuse Act 1990 / Serious Crime Act 2015
- Protection of Children Act 1978
- Obscene Publications Act 1959 and 1964
- Sexual Offences Act 2003
- Data Protection Act 2018
- The Counter-Terrorism and Security Act (2015) / CONTEST (Jun 2018)

2) USE OF COMPUTER EQUIPMENT

In order to control the use of UKTD's computer systems and equipment and reduce the risk of contamination or misuse, the following will apply:

a) the introduction of new software must first of all be checked and authorised by the IT Team Leader before general use will be permitted;

b) only authorised staff should have access to UKTD computer equipment;

c) only authorised software may be used on UKTD computer equipment;

d) only software that is used for business applications may be used;

e) no software may be brought onto or taken from UKTD premises without prior authorisation;

f) unauthorised access to the network system will result in disciplinary action;

g) unauthorised copying and/or removal of computer equipment/software will result in disciplinary action; such actions could lead to dismissal.

UKTD staff are required to not:

- Use other people's passwords or login identities.
- Change, copy, corrupt or destroy any other user's data.
- Deliberately introduce viruses, worms, Trojans or other harmful or nuisance programmes/files on to UKTD systems.
- Install, remove or copy software.

3) VIRUS PROTECTION PROCEDURES

In order to prevent the introduction of virus contamination into the software system the following must be observed:

- unauthorised software including public domain software, USB drives, external hard drives, CDs or internet downloads must not be used;
- all software must be virus checked using standard testing procedures before being used.

4) INTERNET & EMAIL POLICY

The purpose of the Internet and Email Policy is to provide a framework to ensure that there is continuity of procedures in the usage of internet and email within the Company.

Use of the INTERNET

The internet should be used for official and professional activities such as research and finding sites that help in the completion of work. Sites that require payment for services should not be accessed, unless appropriate authorisation has been given.

Attention must be paid to ensuring that published information has relevance to normal professional activities before material is released in the UKTD name. Where personal views are expressed, a disclaimer stating that this is the case should be clearly added to all correspondence. The intellectual property right and copyright must not be compromised when publishing on the internet.

The availability and variety of information on the internet has meant that it can also be used to obtain unsuitable or offensive material. The use of the internet to access and/or distribute any kind of offensive material, or material that is not work-related, leaves an individual liable to disciplinary action which could lead to dismissal. Should unsuitable sites be accessed inadvertently, please report to your line manager.

Acceptable / Unacceptable Use of the Internet

The internet is available for legitimate business use and matters concerned directly with the job being done. Employees using the internet system should give particular attention to the following points:

i. comply with UKTD policy standards;

ii. access during regular working hours should be for business use only;

iii. private use of the internet should be kept to a reasonable level during your normal working day, for example during breaks or lunch time.

UKTD will not tolerate the use of the internet for unofficial or inappropriate purposes, including:

i. accessing websites which put our network at risk of (including but not limited to) viruses, compromising our copyright or intellectual property rights;

ii. creating, copying, sending, storing, displaying or receiving:

   a. Any offensive, obscene or indecent images, data or other material. (It is ILLEGAL to view indecent images of children.)

   b. Material which is designed or likely to cause upset, annoyance, inconvenience or needless anxiety.

   c. Material which could be considered menacing, discriminatory, harassing, bullying, fraudulent or confidential/private.

   d. Material that is for "leisure activity" (eg playing games) unless this is an integral part of the course. This includes online gambling sites.

   e. Material that infringes the copyright of another person, including unlicensed or illegal software.

   f. Defamatory or libellous material.

   g. Inappropriate material to any other network users or distribution lists that waste network resources.

   h. Material that involves extremist organisations or promotes beliefs contrary to British values, as required under the UK Government Prevent Strategy.

iii. engaging in computer hacking and other related activities, or attempting to disable or compromise security of information contained on UKTD computers.

Unauthorised or inappropriate use of the internet system may result in disciplinary action which could result in dismissal.

Use of EMAIL

The use of the email system is encouraged as its appropriate use facilitates efficiency and assists UKTD staff in carrying out their work. Appropriate use is for communication and matters directly concerned with the legitimate UKTD business. Inappropriate use however causes many problems including distractions, time wasting and legal claims.

Authorised Use of Emails

Employees using the email system should give particular attention to the following points:

i. all emails comply with Company communication standards;

ii. email messages and copies should only be sent to those for whom they are particularly relevant;

iii. email should not be used as a substitute for face-to-face communication or telephone contact. Abusive emails must not be sent. Hasty messages sent without proper consideration can cause upset, concern or misunderstanding;

iv. if the email is confidential the user must ensure that the necessary steps are taken to protect confidentiality. The Company will incur liability for infringements of copyright or any defamatory information that is circulated

either within the Company or to external users of the system;

v. offers or contracts transmitted by email are as legally binding on the company as those sent on paper.

UKTD will not tolerate the use of the email system for unofficial or inappropriate purposes, including:

i. any messages that could constitute bullying, harassment or other detriment;

ii. personal use (e.g. social invitations, personal messages, jokes, cartoons, chain letters or other private matters);

iii. online gambling;

iv. accessing or transmitting inappropriate, illegal or offensive material;

v. transmitting copyright information and/or any software available to the user;

vi. posting confidential information about the Company, other employees, our learners, employer partners or suppliers.

Unauthorised or inappropriate use of the email system may result in disciplinary action which could include dismissal.

- **Inappropriate content** includes: pornography, racial or religious slurs, gender-specific comments, information encouraging criminal skills, terrorism or radicalisation, or materials relating to cults, gambling and illegal drugs.
- This definition of inappropriate content or material also covers any text, images or other media that could reasonably offend someone on the basis of race, age, sex, religious or political beliefs, national origin, disability, sexual orientation, or any other characteristic protected by law.

5) SOCIAL NETWORKING SITES

Any work related issue or material that could identify an individual who is a learner, work colleague or employer partner, or which could adversely affect the Company, must not be placed on a social networking site. This means that work related matters must not be placed on any such site at any time either during or outside of working hours and includes access via any computer equipment or mobile device.

Use of Personal Social Media Accounts at Work

Acceptable use:

i. Staff may use their personal social media accounts for work-related purposes during regular hours, but must ensure this is for a specific reason (eg competitor research). Social media should not affect the ability of employees to perform their regular duties.

ii. Use of social media accounts for non-work purposes is restricted to non-work times, such as breaks and during lunch.

iii. Staff must not use their personal social media accounts to contact learners.

Employees should ensure it is clear that their social media account does not represent the Company's views or opinions.

Safe Responsible Social Media Use

The rules in this section apply to:

- Any employees using Company social media accounts
- Employees using personal social media accounts during company time

Users Must Not:

i. Create or transmit material that might be defamatory or incur liability for the Company.

ii. Post messages, status updates or links to material or content that is inappropriate.

iii. Use social media for any illegal or criminal activities.

iv. Send offensive or harassing material to others via social media.

v. Broadcast unsolicited views on social, political, religious or other non-business related matters.

vi. Send or post messages or material that could damage the Company's image or reputation.

vii. Interact with UKTD competitors in any way which could be interpreted as being offensive, disrespectful or rude. (Communication with direct competitors should be kept to a minimum.)

viii. Discuss colleagues, competitors, employers or suppliers without their approval.

ix. Accept learners as 'friends' on Facebook or other social networking sites.

x. Post images or speak about learners on UKTD social media accounts without their full permission and completion of a UKTD Social Media Consent form.

xi. Post, upload, forward or link to spam, junk email or chain emails and messages.

EXAMPLES OF BREACHES OF THIS POLICY

- Sending of nuisance email.
- Unauthorised access through use of another user's credentials.
- Sending abusive, harassing, offensive or intimidating email.
- Maligning, defaming, slandering, or libelling another person.
- Misuse of software or software licence infringement.
- Loading, viewing, storing or distributing inappropriate or other offensive material.
- Unauthorised, copying, storage or distribution of software.
- Any action whilst using UKTD property deemed to bring UKTD into disrepute.
- Attempting to modify, damage circumvent or destroy IT systems security.
- Attempting to use UKTD ICT facilities, systems and/or resources to communicate with or draw people into acts of terrorism/extremism.

CONSEQUENCES OF A BREACH

In the event of a known or suspected breach of this policy, UKTD will take action to manage the security and accessibility of IT computing and ICT resources.

A breach of the ICT Acceptable Use Policy will be dealt with according to its severity. This may lead to formal disciplinary action and in extreme circumstances the police may be called.

Employees that identify a suspected breach of the ICT Acceptable Use Policy are responsible for reporting the incident immediately to their line manager and preserving any evidence.

AUDITING & PRIVACY

UKTD uses content filters and firewalls and block inappropriate usage of ICT equipment.

UKTD reserve the right to:

Carry out conduct checks on internet usage and user files stored on the shared drive or devices, for the purposes of investigating suspected breaches of the ICT Acceptable Use Policy or to comply with safeguarding and Prevent duty responsibilities.

RELATED POLICIES & PROCEDURES

HS0004	UKTD Safeguarding Policy
HS0005	UKTD Safeguarding Procedure
HS0007	UKTD Prevent Policy
PP0047a	UKTD Whistleblowing Policy
PP0059	UKTD Data Protection Policy (GDPR)
HR0003	UKTD Employee Handbook

Acceptable ICT Use for

UKTD Learners

ACCEPTABLE ICT USE FOR LEARNERS

UKTD provides apprentices and learners with access to ICT equipment and systems to support you in your learning, help develop your skills for the future, gain experience of industry standard software and become confident in the use of ICT.

The aim of this guidance is to: -

- Maintain the security of UKTD IT systems.
- Support an effective teaching and learning environment for all UKTD learners.
- Ensure that users do not use UKTD IT systems to break the law.
- Help learners stay safe online and safeguard from harm or IT-based threats.

These guidelines apply to all computers, mobile devices, software and data belonging to UKTD. It includes the use of our ePortfolio system and covers remote access regardless of which device is used to make the connection e.g. personal computer at home, computers at work or mobile phone. These resources are provided on the understanding that they are not misused in any way that will interfere with, disrupt or prevent anyone from legitimately using UKTD resources.

You may not use UKTD systems for creating, copying, sending, storing, displaying or receiving:

- Any offensive, obscene or indecent images, data or other material.
- Material which is designed or likely to cause upset, annoyance, inconvenience or needless anxiety.
- Material which could be considered menacing, discriminatory, harassing, bullying, fraudulent or confidential / private.
- Material that is for "leisure activity" (e.g playing games) unless this is an integral part of the course.
- Material that infringes the copyright of another person, including unlicensed or illegal software.

You must not create, run, send, store or transmit:

- Defamatory or libellous material.
- Unsolicited commercial or advertising material.
- Inappropriate material to any other network users or distribution lists that waste network resources.

Learners are also required to not:

- Use other people's passwords or login identities.
- Change, copy, corrupt or destroy any other user's data.
- Deliberately introduce viruses, worms, Trojans or other harmful or nuisance programmes or files on to UKTD systems.
- Install, remove or copy software.
- Use UKTD IT systems in a manner that could be reasonably regarded as being discriminatory based on race, religion, belief, gender, sexual orientation, gender reassignment, age, or disability.

UKTD reserves the right to define all terms (e.g. menacing, indecent, defamatory and libellous) in the light of current legal and best industry practice standards.

Please note that it is ILLEGAL to view indecent images of children, access material that involves extremist organisations and/or promotes beliefs contrary to British values, as required under the UK Government Prevent Strategy.

