Online Safeguarding Policy

Statement of Intent

This policy will outline the broad scope of Online Safety for both students and staff whether working in the business or from home. The safety and wellbeing of learners and staff is paramount and this policy aims to ensure online safety is understood and adhered to by the entire college community; as with all safeguarding, online safety is everyone's responsibility.

It is important to share with the learners the underpinning knowledge and behaviours that can help navigate the online world safely and confidently. With this in mind the college will provide the most appropriate software technology, the staff will be trained in delivering lessons safely and the students and staff will be taught how to keep themselves safe online. Everyone will be kept up-to-date with online risks.

1. Introduction and Purpose

1.1. ITEC recognises the benefits and opportunities which new technologies offer to teaching and learning. Our approach is to implement and embed safeguards within the business, and to support staff and learners to identify and manage risks. We believe this can be achieved through a combination of security measures, training and guidance and implementation of our associated policies. As part of our duty to safeguard learners, we will do all that we can to make our learners and staff stay 'e-safe' and to satisfy our wider duty of care. This online safety policy should be read in conjunction with other relevant policies procedures such as Safeguarding, IT e-safety policy and the Harassment and Anti - Bullying Policy, as well as the Blended Learning Policy.
This policy applies to all ITEC stakeholders (including staff, students, parents/carers and visitors) who have access to and are users of the businesses IT systems both in and out of the designated premises.

2. What is Online Safety?

The term online safety is defined for the purposes of this document as the process of limiting the risks to children, young people and vulnerable Adults when using Internet, Digital and Mobile Technologies (IDMTs) through a combined approach to policies and procedures, infrastructures and education, including training, underpinned by standards and inspection. Online safety risks can be summarised under the following three headings.

2.1. Content • Exposure to age-inappropriate material • Exposure to inaccurate or misleading information • Exposure to socially unacceptable material, such as that inciting violence, hate, extremism or intolerance • Exposure to illegal material, such as images of child abuse • Illegal Downloading of copyrighted materials e.g. music and films
2.2. Contact • Grooming using communication technologies, potentially leading to sexual assault or child prostitution • Radicalisation the process by which a person comes to support terrorism and extremist ideologies associated with terrorist groups. • Bullying via websites, mobile phones or other forms of communication device
2.3. Commerce • Exposure of minors to inappropriate commercial advertising • Exposure to online gambling services • Commercial and financial scams

3. Legal Background or Relevant Legislation and Guidance

3.1. The Education and Inspections Act 2006 empowers organisational leaders to such extent as is reasonable, to regulate the behaviour of students when they are off site, for example if students are involved in incidents of cyber-bullying or other online safety incidents covered by this policy and which may take place outside of the college but is linked to membership of the college, they can be subject to the college disciplinary procedure.

3.2. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data (see appendix for template policy). In the case of both acts, action can only be taken over issues covered by the published Behaviour Policy.

4. Scope of the Policy

ITEC will deal with issues related to inappropriate online behaviour within this policy and associated behaviour and anti-bullying polices and will, where appropriate, inform parents/carers. When necessary the appropriate external agencies (such as the police) will also be informed.

Learners are taught

a. Online safety and risk of harm. This will include being taught what positive, healthy and respectful online relationships look like, the effects of their online actions on others and knowing how to recognise and display respectful behaviour online.
b. How to use technology safely, responsibly, respectfully and securely, and where to go for help and support when they have concerns about content or contact on the internet or other online technologies.
c. How to evaluate what they see online - this will enable pupils to make judgements about what they see online and not automatically assume that what they see is true, valid or acceptable.
d. How to recognise the techniques that are often used to persuade or manipulate others and understanding that a strong grasp of knowledge across many areas makes people less vulnerable to these techniques and better equipped to recognise and respond appropriately to grooming or malicious activity.
e. Be able to identify possible online risks and make informed decisions about how to act; help students assess a situation, think through possible conseqences and decide on the best course of action.
f. Online relationships, healthy relationships, privacy and security, online reputation and online bullying
g. Vulnerable students may be more susceptible to online harm and are more closely supported with all of the above plus more regular check-ins with staff so that positive relationships are built swiftly
h. GDPR legislation and guidance

Staff are trained to

i. To be aware of current risks posed online
j. To be confident in their knowledge of online safety
k. To spot issues
l. To deliver online lessons safely
m. Deliver online safety information and guidance to parents/carers
n. GDPR guidance and legislation

5. Safeguarding

5.1. Radicalisation

5.1.1. Radicalisation refers to the process by which a person comes to support terrorism and forms of extremism. Learners must report to any member of staff if they view any extremist or radical views expressed online. Staff should report any concerns immediately to a member of the safeguarding team.

5.1.2. There is no single way of identifying an individual who is likely to be susceptible to an extremist ideology. It can happen in many different ways and settings. Specific background factors may contribute to vulnerability which are often combined with specific influences such as family, friends or online, and with specific needs for which an extremist or terrorist group may appear to provide an answer.

5.1.3. The Internet and the use of social media in particular has become a major factor in the radicalisation of young people.

5.1.4. "Radicalised learners can also act as a focal point for further radicalisation through personal contact with fellow learners and through their social media activity. Where radicalisation happens off campus, the learner concerned may well share his or her issues with other learners. Changes in behaviour and outlook may be visible to staff. ITEC will self-assess and identify the level of risk, ensure all staff have access to training, and that there is welfare support for learners and effective IT policies in place which ensure that these signs can be recognised and responded to appropriately".

"Institutions must have clear policies in place for students and staff using IT equipment to research terrorism and counter terrorism in the course of their learning". (Prevent Duty Guidance: for further education institutions in England and Wales 2015)

5.2. Child Exploitation

5.2.1. Child Sexual Exploitation (CSE) may involve utilising the Internet and Social Media to identify potential victims or as a tool to coerce and blackmail children into performing sexual acts, both on and offline.

5.2.2. Means of accessing the Internet may also be provided to children as a "gift" by perpetrators such as in the form of new mobile phones and devices. In some cases, CSE can take place entirely online such as children and young people being coerced into performing sexual acts via webcam/Social Media and therefore may not always result in a physical meeting between children and the offender.

5.2.3. "Section 39. Sexual abuse: involves forcing or enticing a child or young person to take part in sexual activities, not necessarily involving a high level of violence, whether or not the child is aware of what is happening. The activities may involve physical contact, including assault by penetration (for example rape or oral sex) or non-penetrative acts such as masturbation, kissing, rubbing and touching outside of clothing. They may also include non-contact activities, such as involving children in looking at, or in the production of, sexual images, watching sexual activities, encouraging children to behave in sexually inappropriate ways, or grooming a child in preparation for abuse (including via the internet). Sexual abuse is not solely perpetrated by adult males. Women can also commit acts of sexual abuse, as can other children." (Keeping Children Safe In Education, September 2018, section 39)

5.3. Youth Produced Sexual Imagery and Sharing of Inappropriate Imagery

5.3.1. Youth Produced Sexual Imagery (YPSI – formerly known as 'Sexting') can be defined as 'an increasingly common activity among children and young people, where they share inappropriate or explicit images online'. This can include sharing indecent images of themselves or others via mobile phones, webcams, social media and instant messaging.

5.3.2. "Section 41. All staff should have an awareness of safeguarding issues. Staff should be aware that behaviours linked to the likes of drug taking, alcohol abuse, truanting and YPSI put children in danger." (Keeping Children Safe In Education, September 2018, section 41)

5.3.3. Although viewed by many young people as a 'normal' or 'mundane' activity and part of 'flirting', YPSI can be seen as harmless; but creating or sharing explicit images of a child is illegal, even if the person doing it is a child. A young person is breaking the law if they:

5.3.3.1. take an explicit photo or video of themselves or a friend;

5.3.3.2. share an explicit image or video of a child, even if it's shared between children of the same age;

5.3.3.3. possess, download or store an explicit image or video of a child, even if the child gave their permission for it to be created.

5.3.4. "Section 42. All staff should be aware safeguarding issues can manifest themselves via peer on peer abuse. This is most likely to include, but not limited to: bullying (including cyber bullying), gender based violence/sexual assaults and YPSI. Staff should be clear as to the school or college's policy and procedures with regards to peer on peer abuse." (Keeping Children Safe In Education, September 2018, section 42)

5.3.5. ITEC utilises the CEOP (Child Exploitation & Online Reporting Centre) reporting button, which is available on all student machines and the College website. The implementation of this button allows students to be empowered to report suspicious individuals or activity directly to law enforcement professionals quickly and easily. DO WE ?

6. Social media

6.1. Social media is a useful tool; ITEC understand that students communicate and collaborate via sites and apps on a regular basis positively.

6.2. Unfortunately, there are also risks attached to the use of social media; everyone at ITEC is expected to use it responsibly, inside and outside of the campus. Learners should report offensive or inappropriate messages to a member of staff

7. Accessing the Internet on College premises: Monitoring & Filtering

7.1. The Internet is available on all ITEC systems to help students with their studies. Whilst it is essential that appropriate filters and monitoring processes are in place, ITEC recognises that 'over blocking' does not lead to reasonable restrictions and does not replace what young people are taught with regards to online safety and safeguarding. Students must immediately tell a member of staff if they think their network account has been tampered with.

7.2. All the websites visited and unencrypted online content are automatically logged by Internet monitoring software including Sophos. This uses advanced techniques such as URL Reputation and Automatic Image Recognition technology. In addition, it can also monitor Cloud application activity such as WhatsApp/ Facebook / Instagram and more. Both on College computers and on Wi-Fi.

7.3. As members of the Internet Watch Foundation (IWF), Sonicwall and Fastvue adhere to strict guidance in order to block access to illegal Child Abuse Images and Content (CAIC) and integrate the CITRU block-list (a police assessed list of unlawful terrorist content, produced on behalf of the Home Office).

7.4. Sonicwall may block access to some sites; if such a site is related to a student's normal working requirements please contact the ICT Helpdesk to arrange for the site to be reviewed and unblocked (where permissible).

7.5. Uploading and/or circulation of derogatory or defamatory comments and/or images about the ITEC and/or its staff and/or students to any internet service (websites, social media, etc) is not permitted. Abuse of the Internet facilities will be seen as improper use of ITEC equipment and will lead to disciplinary procedures

7.6. ITEC has implemented content filters to prohibit access to the categories listed below. Any student found attempting to access inappropriate or harmful material will be subject to the Disciplinary procedures. This list is updated regularly:

- **7.6.1.** Discrimination: Promotes the unjust or prejudicial treatment of people on the grounds of race, religion, age or sex
- **7.6.2.** Drugs/Substance abuse: Displays or promotes the illegal use of drugs or substance
- **7.6.3.** Extremism: Promotes terrorism and terrorist ideologies, violence or intolerance
- **7.6.4.** Malware/Hacking: Promotes the compromising of systems including anonymous browsing and other filter bypass tools as well as sites hosting malicious content
- **7.6.5.** Pornography: displays sexual acts or explicit images
- **7.6.6.** Piracy and copyright theft: Includes illegal provision of copyrighted material
- **7.6.7.** Self-Harm: Promotes or displays deliberate self-harm (including suicide and eating disorders)
- **7.6.8.** Violence: Displays or promotes the use of physical force intended to hurt or kill

N.B. This list is not exhaustive

8. Data Protection

8.1. ITEC will comply with the Data Protection Act 2018 and GDPR by ensuring that personal data is:

- **8.1.1.** Collected and processed lawfully, fairly and transparently for only specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.
- **8.1.2.** Adequate, updated and relevant and not excessive for the purposes it was collected.
- **8.1.3.** Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures. Including not being transferred to a country outside the European Economic Area, unless that country has equivalent levels of protection for personal data.
- **8.1.4.** Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals.

9. Confidentiality

9.1. The Data Protection Act 2018 is the UK's implementation of the General Data Protection Regulation (GDPR). The General Data Protection Regulation (GDPR) replaced the Data Protection Act 1998 in the UK. It is part of the wider package of reform to the data protection landscape that includes the Data Protection Bill. The GDPR sets out requirements for how organisations will need to handle personal data from 25 May 2018.

9.2. These are not only restrictions on disclosure of information about ITEC, they are bound by a common law duty of confidentiality. This duty prevents ITEC from releasing information about staff and learners, without their consent. This duty applies to manual records as well as information held on computers.

9.3. Information which must be treated as confidential includes the names and addresses of employees and students and any other information about them which is not publicly known aka "personal data". Accordingly, to ensure that we do not breach our duty, no information, even if it only exists in printed form, should be disclosed unless all the relevant procedures have been followed.

9.4. Since 1 January 2005 people have the right, under the Freedom of Information Act 2000, to request any information held by a public authority which it has not already made available through its publication scheme. Please see the Freedom of Information -A guide to the publication scheme (January 2009), which is available on the College groups website, for more information.

Online Safeguarding Policy

1. Linked Policies

a. ITEC ingle Equality Scheme
b. Safeguarding Policy
c. Behaviour Policy
d. Staff e-safety Policy
e. Blended Learning Policy
f. Acceptable Use Policy
g. Email Policy
h. Mobile Phone Policy

2. Responsibilities – Nominated Persons

The following section outlines the roles and responsibilities of individuals and groups within ITEC and the USP College Group.

Policy & Procedures Committee:

Responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy. This will be carried out by the committee members receiving regular information about online safety incidents and annual monitoring reports. The Safeguarding Manager will work with the Online Safety Coordinator to review updates to this policy and review monitoring systems relating to this policy

Incidents of inappropriate online behaviour will be dealt with in line with the ITEC disciplinary procedure, parents/carers informed and where necessary appropriate external agencies will be notified

Delivery of online safety to all students – Progress Coaches

Ensure all staff are regularly trained in current online risks – CPD Manager
Ensure all teaching staff are training in delivering safe online lessons – ITEC TIP (see Blended Learning Policy)
Safeguarding concerns are immediately reported to the senior management team in line with safeguarding procedure

3. Monitoring, Review and Evaluation

This policy was approved by the Policies and Procedures Committee on the 23rd February and the implementation of this policy will be monitored by the ITEC management team. Monitoring will take place on a yearly basis.

ITEC will also review the policy to take account of any new Government legislation, regulations or best practice documents, to ensure that staff are kept fully up to date with their responsibilities and duties with regard to these procedures.

ITEC will monitor the impact of the policy using logs of reported incidents (Sophos), reviews of the current software provision, student and staff feedback opportunities via the wider College Group.

Online Safeguarding Policy

Action Plan:

Training for learners on online safety
Update learner handbook
Join up safeguarding process and IAG with College Group

Last Reviewed	23 February 2021
Reviewed by	Ben Turner