PROGRESSIVE CONSULTANCY AND TRAINING

Acceptable Use of IT Policy and Procedure

Modification Overview:

Author:	Oliver Saunders
Edited Author:	Angela Saunders, Oliver Saunders
Date of Approval:	28/03/2024
Next Review:	29/03/2025

Address:	Allard House 38 Moor Street Earlsdon Coventry CV5 6EQ
Designated Safeguarding Lead: (DSL):	Angela Saunders

Policy Title:	Acceptable Use of IT Policy

Version:	2.0
Links:	Policies: 16, 29, 38, 43

Disclosure:

Progressive Consultancy and Training (PCT) seeks to take all reasonable steps to help ensure that it follows all policy and procedures that are outlined within this document. This policy is supported by robust procedures and appropriate guidance and can therefore be used in conjunction with other stated policies and procedures. Further information can be found on the PCT website or when contacting Angela Saunders or another member of PCT staff.

1. Purpose

1.1. The continued integration of Information Technology (IT) in the curriculum presents both an opportunity and risk for students' development, and so requires that centre administrators, teachers, students, parents, and carers take steps to ensure that IT is used responsibly at the centre.

The Policy aims to ensure and promote the safe use of IT, both during use at the centre, and outside of education, avoiding illegal and inappropriate content for the continued safeguarding of students.

The full form of IT is Information Technology. IT is used in the context of computers. The IT sector uses software and computers to handle information. Computer software and electronic computers are used here to transform, secure, and store information and data.

2. Rationale

2.1. Aspects of the curriculum may require the use of IT such as laptops or computers, tablets, or other connected devices. Some of this use may involve the connection to the internet, and so there is the need to manage any risk to students and staff during the use of IT.

2.2. Despite best efforts to implement and enforce safeguarding restrictions on IT, PCT acknowledges that in the dynamic state of the internet and other connective services, that there still remains a risk to the safeguarding of students during the use of IT.

3. Responsibility

3.1. It is the responsibility of students and staff who use IT within the centre to abide by the guidelines outlined in this document.

3.2. Parents/carers should be aware of the Acceptable Use Policy and engage with staff in ensuring safe and appropriate use of IT.

3.3. It will be the teaching staff member's responsibility to take action should students breach the Policy, and take correct steps for reporting and investigation. Students will be reminded of the Policy before first use of IT.

3.4. Senior Leadership will be responsible for the monitoring and response to breaches of the Policy, and for the referral to external agencies if necessary.

3.5. It will be the responsibility of Senior Leadership to designate a member of staff to ensure that IT is kept up to date with the appropriate safeguards, such as Anti-Virus and Restrictive Filtering Controls, to prevent the inappropriate and unsafe use of IT.

4. Acceptable Uses

4.1. Students should ensure that IT is only used under the instruction of staff, and use does not deviate from the initial requirements of use.

4.2. All use of IT when instructed under free use should remain appropriate for the context of users in an education environment.

4.3. IT should be reserved for personal use only, unless instructed otherwise by staff, and students should avoid showing other students their own device to prevent the accidental exposure of inappropriate material.

5. Unacceptable Uses

5.1 The following are deemed as unacceptable:

- Using any application or service that bypasses the filters and security measures imposed by the Centre.
- Using Centre IT to run a private business.
- Revealing or publishing confidential or proprietary information (e.g. financial or personal information, network access information etc.).
- Creating or spreading malware and other harmful files.

5.2. Students are also completely prohibited from using internet-connected IT services to search for or obtain material on pornography, threatening behaviour such as violence or mental harm, the infringement of copyright or licensing, the promotion of extremism or terrorism, or any other material which may undermine the ethos or integrity of the Centre.

5.3. Visiting websites, making, posting, downloading, uploading, data transferring, communicating, or passing on material, remarks, proposals or comments that relate to or contain the following are also deemed as unacceptable and illegal:

- Child sexual abuse images - The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978.
- Grooming, incitement, arrangement or facilitation of sexual acts against children. Contrary to the Sexual Offences Act 2003.
- Possession of an extreme pornographic image. Contrary to the Criminal Justice and Immigration Act 2008.
- Criminally racist material in the UK to stir up hatred based on religion or sexual orientation. Contrary to the Public Order Act 1986.

5.4. The use of IT must not disrupt classroom lessons with audio, music, or beeping. This includes the use of SMART watches that are linked to other devices, such as a mobile phone (please refer to our mobile phone policy).

5.5. Using IT to bully and threaten other students is unacceptable and will not be tolerated. In some cases it can constitute criminal behaviour.

5.6. Students are not to alter or delete other students' work or learning resources.

6. Theft or damage

6.1. Students should only use IT with the supervision or permission of a member of staff, this is to allow staff to account for the whereabouts and last users of all IT at all times.

6.2. Should the use of IT include the use of students' personal mobile phones, the Mobile Phone Policy and Procedure apply in regards to acceptable use as well as theft or damage.

6.3. Any damage to IT equipment during use is to be reported to a member of staff immediately to allow the assessment of damage and any safety risk to students in the event of electrical damage or otherwise.

7. Inappropriate conduct and Sanctions

7.1. Any students using IT equipment to cheat in exams or assessments will face disciplinary action as sanctioned by the Centre Head.

7.2. Any student who carries out any action as detailed in *5. Unacceptable Uses* will face disciplinary action as sanctioned by the centre head.

7.4 Failure to hand over or seize use of IT equipment when requested will escalate the sanctions to Stage 2 immediately and a referral to the council team and referring school. If the reason for this request is related to points raised in Section 5.3, then it may be necessary for the Centre Head to involve relevant third party authorities, such as the police.

8. Process for Handling Safety Incidents

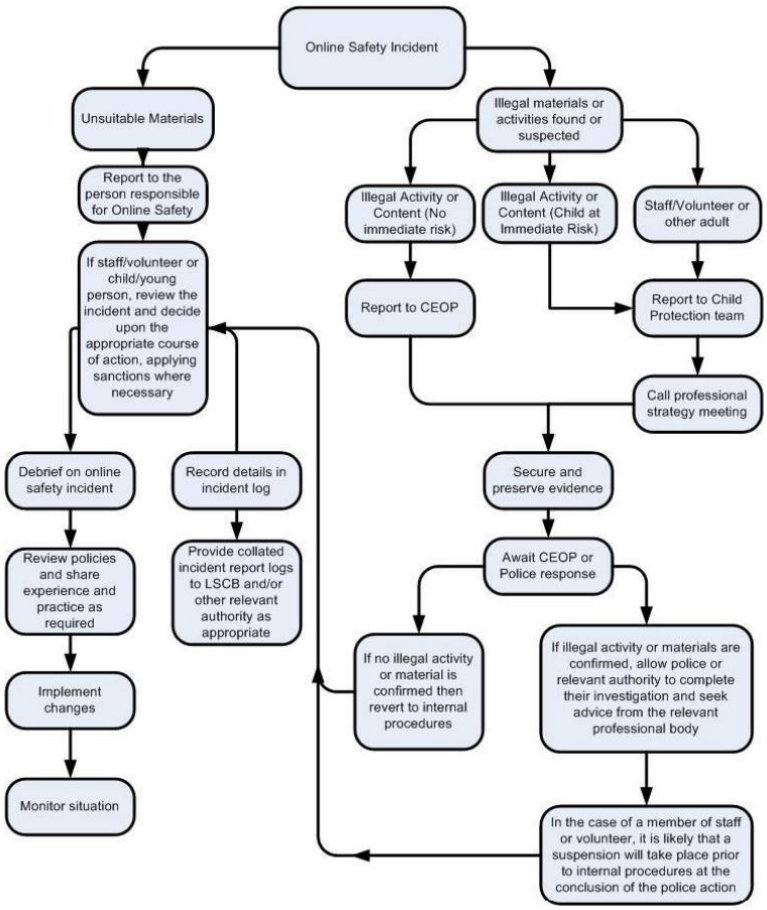
8.1. The flowchart procedure as shown in Section 8.2. must be followed in handling incidents of risk to online safety, and the following measures must be adopted to ensure good practice:

- Designate more than one member of staff in the investigation of incidents. This is to protect individuals, if accusations are subsequently reported.
- Conduct investigative procedures using a designated computer, which cannot be accessed by students or related staff, which can also be taken off site if needed by external authorities such as the police. Use the same computer for the entire procedure.
- All investigative staff should be allowed access to the internet for the purposes of the investigation, but the content viewed and any websites visited should be monitored and recorded in the interest of the protection of the investigative individual.
- Record the URL and content of the suspected misuse, it may also be necessary to

obtain screenshots or records of the content on the designated device used in the investigation. In the case of child sexual abuse, this does not apply and the below applies instead.

- In the case of content related to child sexual abuse, monitoring should be immediately halted and referred to the Police (CEOP). Other instances to report to the Police immediately include: Grooming behaviour, the sending of obscene images to a child, adult material which potentially breaches the Obscene Publications Act, criminally racist material, promotion of terrorism or extremism, other criminal conduct, activity or material.
- Once monitoring is complete and investigation has taken place, investigative staff will need to make a judgement as to whether the concern has substance and if further action is required, and to what extent, such as: Internal response as outlined in Child Protection and Safeguarding Policy and Behaviour Policy, involvement of the Local Authority (in the form of the Local Safeguarding Children Board (LSCB), Multi Agency Safeguarding Hub (MASH), or otherwise), other relevant organisations, or Police involvement.
- The device in question should be isolated as best as possible, as any further use or alteration to the device may hinder a later police investigation. This isolation should remain in place until an outcome is achieved and is then approved for reuse by the Centre Head.

8.2. The following flowchart must be followed with the points raised in Section 8.1. considered at all times.



Contacts

If you have any queries or concerns regarding these policies / procedures then please contact Angela Saunders, Director.