Treloar's
Enabling Education

Policy/Procedure Name:	E-safety Policy
Policy/Procedure Number:	ICT 004
Date of Approval:	October 2008
Effective Date:	October 2008
Revised Date:	December 2023
Review by Date:	December 2025
Policy/Procedure Author:	Head of Learning Technology
Policy/Procedure Owner:	Principal
Management Committee Approved By:	TLT
Governor /Trustee Committee Approved By (where appropriate):	N/A
For Action By:	All Staff
For Information to:	Staff, Students, Parents, Governors
Approval requested to upload on the Treloar Website:	Yes ☑ (tick if requested)

Who is carrying out EIA? (see details of EIA in appendix)	Jo Cox	Date of EIA?	Sept 22

Aim

Information and communication technology (ICT) has changed the way we learn, work and live and will continue to do so. The future impact of ICT on students, staff and volunteers working at Treloar's and on families and students as they move into adulthood, cannot be foreseen. What is certain is that young people with disabilities must be given the confidence, motivation and skills to harness technology if they are to benefit from its advances and not be disadvantaged by comparison with their non-disabled peers. This procedure aims to provide levels of protection appropriate to age, vulnerability and cognitive skills and complying with all legal requirements.

1. The Range of the Policy

This policy applies to the Treloar's ICT network. There are three key elements of the e-safety policy:

- Whole organisation awareness, designated responsibilities, policies and procedures
- An effective range of technological tools
- A comprehensive Internet safety education programme

2. Whole organisation awareness

Awareness of eSafety issues and their potential impact is raised through staff training and a comprehensive eSafety education programme for students. These respond to specific incidents and issues and are updated periodically to take account of changing technologies.

2.1 Designated Roles and Responsibilities

E-Safety is an essential aspect of SMT and the Governors who ensure that they embed safe practices into the culture of each of their areas of responsibility.

2.2 Filtering

The Trust takes all reasonable precautions to ensure that users access only appropriate material. It cannot accept liability for the material accessed, or any consequences of Internet access.

The Trust's network is filtered by Smoothwall and protected from virus attack by commercial software. If staff or students discover unsuitable sites, the URL (website address) and content must be reported to the Network Manager or Head of Learning Technology.

2.3 Misuse of ICT services and/or resources

Despite the filtering and the integrity of the system there may still be occasions when misuse of the network or other electronic media occurs. For students, in most cases, the designated member of curriculum staff responsible for ICT should deal with minor incidents. For staff, incidents are reported to the Head of Safeguarding and passed to the staff member's line manager. A warning or suspension of access to the system may be the most appropriate response unless the behaviour is repeated or escalates. The incident and its response should be recorded using IRIS and monitored so that any trends can be identified and necessary action taken. This might include raising awareness among students, staff or parents by meetings, notices or training.

3. Cyber bullying

Cyber bullying is defined as the deliberate use of ICT, particularly mobile phones and the Internet, to harass and bully another individual.

3.1 Prevention

Essential elements of prevention are by raising awareness of the issues and promoting understanding about cyber bullying through staff development, liaison with parents, and curriculum delivery.

3.2 Intervention

Incidents of cyber bullying and action taken will be recorded on IRIS and monitored so that policies and procedures can be evaluated and updated. Any evidence such as texts or emails should be kept to assist in an investigation. Additional sources of evidence may be available through Computer Services, Internet Service providers, Mobile Phone Company or social network sites. Once bullying has been disclosed, it should be dealt with through existing anti-bullying and behaviour policies and the perpetrator identified and sanction applied. Cyber bullying, like all forms of bullying should be taken seriously and is never acceptable.

4. Use of Digital Images

Treloar's is very proud of the achievements of all its learners in their academic, artistic and sporting endeavours. We celebrate our diversity and achievements in many ways, such as displaying photographs of learner's work, team photographs, and trips in which our learners have participated. We make full use of digital signage screens inside the school and college to enhance our displays and our website is updated regularly. Learners are always properly supervised when professional photographers visit the school. Parents are given the opportunity to purchase copies of these photographs.

Whilst images are regularly used for very positive purposes, adults need to be aware of the potential for these to be taken and/or misused or manipulated for pornographic or 'grooming' purposes. Particular regard needs to be given when images are taken of young or vulnerable persons who may be unable to question why or how the activities are taking place. Pupils who have been previously abused in a manner that involved images may feel particularly threatened by the use of photography, filming etc. Staff should remain sensitive to any pupil who appears uncomfortable and should recognise the potential for misinterpretation.

All new staff are given guidance on Trust's policy on taking, using and storing images of learners.

Current staff will be reminded of this guidance at the start of each academic year as follows:

4.1 The School and College will:

- Require parents/guardians or students over 16 who have capacity to provide documented consent before images can be stored or used.
- The naming of published images of students will be avoided wherever possible, unless it's considered necessary, is in the student's best interests and the student and/or parents have consented. Where named images are used then specific written permission from parents or guardians of students under eighteen must be obtained. Documented consent will also be obtained from students over 16 who are competent to give it.
- Recording images of children participating in extracurricular events that are taken for personal use are exempt from the Data Protection Act. These include uses such as parents taking photographs of sports day or videoing a school play, or students using their own phones and cameras as part of normal daily activities and socialisation. The School and College will monitor the use of cameras and anyone behaving inappropriately or worrying others through use may be challenged to change behaviour, cease using the device or leave the premises.
- All students featured in published images (including internal publishing, e.g. on SharePoint or within review reports) must be appropriately dressed with outer clothing garments covering their torso from at least the bottom of their neck to their thighs, (i.e. a minimum of vest/shirt and shorts).
- activities such as swimming, gymnastics and athletics present a higher risk for potential misuse than others, so images of these activities should:
  - focus on the activity being demonstrated, not the body of the student or staff members involved
  - avoid showing the full face and body of a student – instead show students in the water
  - avoid images and camera angles that may be prone to misinterpretation or misuse
  - have consent provided by all in the image (staff or students), acknowledging that individuals may not wish to be photographed, or have these images circulated.
- Where images are taken for medical, health or care purposes (e.g. to allow for documentation and monitoring of skin integrity or posture) they will be securely stored and managed in line with protocol contained in the standard operating procedure for the relevant department.

NB: Staff are forbidden to upload images of students to their social networking sites or to take images of students using their personal mobile phones or personal camera equipment.

Storage and Review

Our images are securely kept on the Trust network, in line with GDPR these are all named with the student’s full name. They are reviewed annually and are deleted when no longer required.

All photographs/videos on cameras and shared devices should be downloaded to the network, named with the student’s full name and stored in the appropriate folder on the shared drive. The photographs should then be permanently deleted from the device

If a camera, tablet, SD card or USB drive with photographs and or videos on is lost by you, this must be reported immediately or as soon as reasonably possible to Computer Services and Head of Technology. Treloar owned staff and student iPads are managed through an MDM server which gives us the ability to disable and wipe any iPad that is lost.

5. Video conferencing and webcams

Webcams are small digital cameras that work with computers and are found on all tablets and smartphones.

5.1 Risks

- Young people can be persuaded to take or send inappropriate photographs or video of themselves, to people they have only had contact with online. Once someone else has the content the young person is at risk of being further manipulated or threatened.
- Webcams use can be difficult to supervise if the computer is in the learner’s bedroom or private space.
- Other learners may be videoed inadvertently by walking past the camera.
- Although fairly rare, there have been cases of people using virus programmes that can hijack the output of a remote webcam and send the images to their own computers.

Webcam in use signs are provide to all departments and these must be displayed on the door when a video conference is taking place.

- All staff need to ensure that when delivering care to the student that all webcams are turned off and any Facetime or Skype conversations are finished.

- All webcams used in class or an open area should be turned off when the session is finished.

- Students and staff supporting them should check whether webcams are enabled prior to offering any care (including medication or nutrition), and establish with the student what their wishes are (or make a best interests decision). This would also include webcams more generally in use in a classroom environment.

The misuse of Webcam, Skype or video conferencing equipment by any learner or member of the Trust will result in disciplinary procedures

6. Internet safety education

E-safety is incorporated into the curriculum for every student at a level appropriate to his or her understanding. In their first year students will take part in Internet Safety sessions, in subsequent years they will undertake a refresher course.

All new staff undertake eSafety training which is updated every three years. Staff are kept appraised of any significant eSafety developments which are passed to them at monthly staff meetings.

6.1 Prevent Strategy

Treloar's School and College has a duty to prevent radicalisation that can lead to violent extremism or terrorism. The internet is a medium that is often used to radicalise people through blogs, social media and other websites and apps. These can be used on fixed and mobile devices that do not always go through Treloar's network and therefore may not be picked up by filters. The duty to prevent will be embedded in esafety as well as safeguarding training. Staff need to be vigilant and report any incident where they see or hear about students access any online (or offline) material that advocates extremist ideas or incites violence and hatred in any way.

7. Social Networking

Social networking refers to a broad range of websites and services that allow people to connect with friends, family, and colleagues online, as well as meet people with similar interests or hobbies.

In line with the Mental Capacity Act, students are considered to have capacity unless the staff supporting the learner, assess that **at the time,** the student has not got the capacity to do so, and a "Best Interests decision is made by supporting staff, not to allow access". In order to comply with the Mental Capacity Act recording requirements, this decision must be recorded in writing with the reason why the access has been denied, signed and dated by the person making that decision. A further capacity assessment must be undertaken if later in that day the student asks again to access a social networking site. It is beyond the authority of a member of staff to deny access to a learner on the grounds of a previously conducted mental capacity assessment

7.1 Student Policy

No access to Social Networking Sites will be given to any learner until:

- They have completed their eSafety programme
- They are over the age of 13.

Action will be taken if any student is found to be using a Social Networking site (either on their phone or on a PC/laptop) to bully another student or staff member.

In the event of a student being contacted by the press about posts on their social networking site that relates them to Treloar's, a member of the SMT must be immediately informed.

If on completion of the eSafety course the tutor delivering the course feels that the student has not fully comprehended or does not have the capacity to understand the issues around eSafety, then, in consultation with the MDT team a tutor will make a professional judgement as to the level of the student's esafety competence using the following scale:

- 0 – 'None' student has no independent access
- 1 – 'Full' student has independent computer access but needs full monitoring to enable safe access
- 2 – ' Significant' – student has independent access but needs regular monitoring and support in ensuring safety
- 3 – 'Moderate' – student has independent access and needs occasional support to ensure safety
- 4 – 'Independent' – student has independent access and is fully aware of e-safety

This information will be documented on Databridge.

If a student who has been assessed at level 1 or 2 wants to access Facebook then a parent/guardian/Social worker will be asked to go through the policy and sign to say that access to Facebook may be given.

7.2 *Staff Policy*

Staff using social networking or social media websites in a manner that can be seen as representing the Trust are required to keep their work and private use of social networking sites separate.

It is against Trust policy to invite current school or college students and or their parents to be a "friend" on their personal social networking site, or accept a friend request from a student or parent. This applies for the first year after they leave Treloars and for any ex-student whilst they remain a child. Staff should be aware that former students, and their friends and families, may themselves be social media friends with current students, and consider appropriate privacy settings

It is also against policy to upload photographs of students to their personal sites.

Staff should ensure that they do not conduct themselves in a way that is and/or could be seen as bringing the Trust into disrepute.

Staff should take care that any activity in which they engage involving ICT, particularly, but not exclusively, on social media websites does not risk bringing Treloar's into disrepute or attract adverse publicity towards Treloar's. In the event of a staff member being contacted by the press about posts on their social networking site that relates them to Treloar's, a member of the SMT must be immediately informed.

Some newly recruited staff may have students as existing friends or contacts on social networking sights such as Facebook. These staff are *not* required to remove the students as friends, but must not add students once they have accepted an offer of employment.

Matters relating to work should not be posted on private social networking sites.

A guide for staff on the safe use of social media can be found here: http://www.childnet.com/ufiles/Social-networking.pdf

Any member of staff who has a concern about the potentially inappropriate use of social networking sites should contact their line manager, the ILT Manager or Computer Services.

8. Blogging

Staff must not use their personal blogs to discuss their work at Treloar's, they must ensure that confidential information is not revealed. This might include aspects of Trust policy or details of internal Treloar discussions.

If a blog makes it clear that the author works for the Trust, it should include a simple and visible disclaimer such as "these are my personal views and not those of Treloar Trust".

Staff members who already have a personal blog or website which indicates in any way that they work for Treloar's, should discuss any potential conflicts of interest with their line manager.

If they are contacted by the press about posts on their blog that relate to the Trust, a member of SMT must be informed.

9. Incident Reporting

E-Safety depends on staff, schools, governors, advisers, parents, and - where appropriate - the pupils themselves taking responsibility. Staff have a particular responsibility to supervise use, plan access and set good examples. The balance between educating pupils to take a responsible approach and the use of regulation is judged carefully.

9.1 Incidents involving others

Any incident involving a member of staff or student is a potentially serious and complex issue. There may be implications for the safety of students, colleagues and the learning environment, and for the reputation of the Trust. ICT related incidents should be recorded and monitored in IRIS and the e-safety and ICT policies reviewed as necessary.

9.2 Safeguarding and dealing with serious incidents

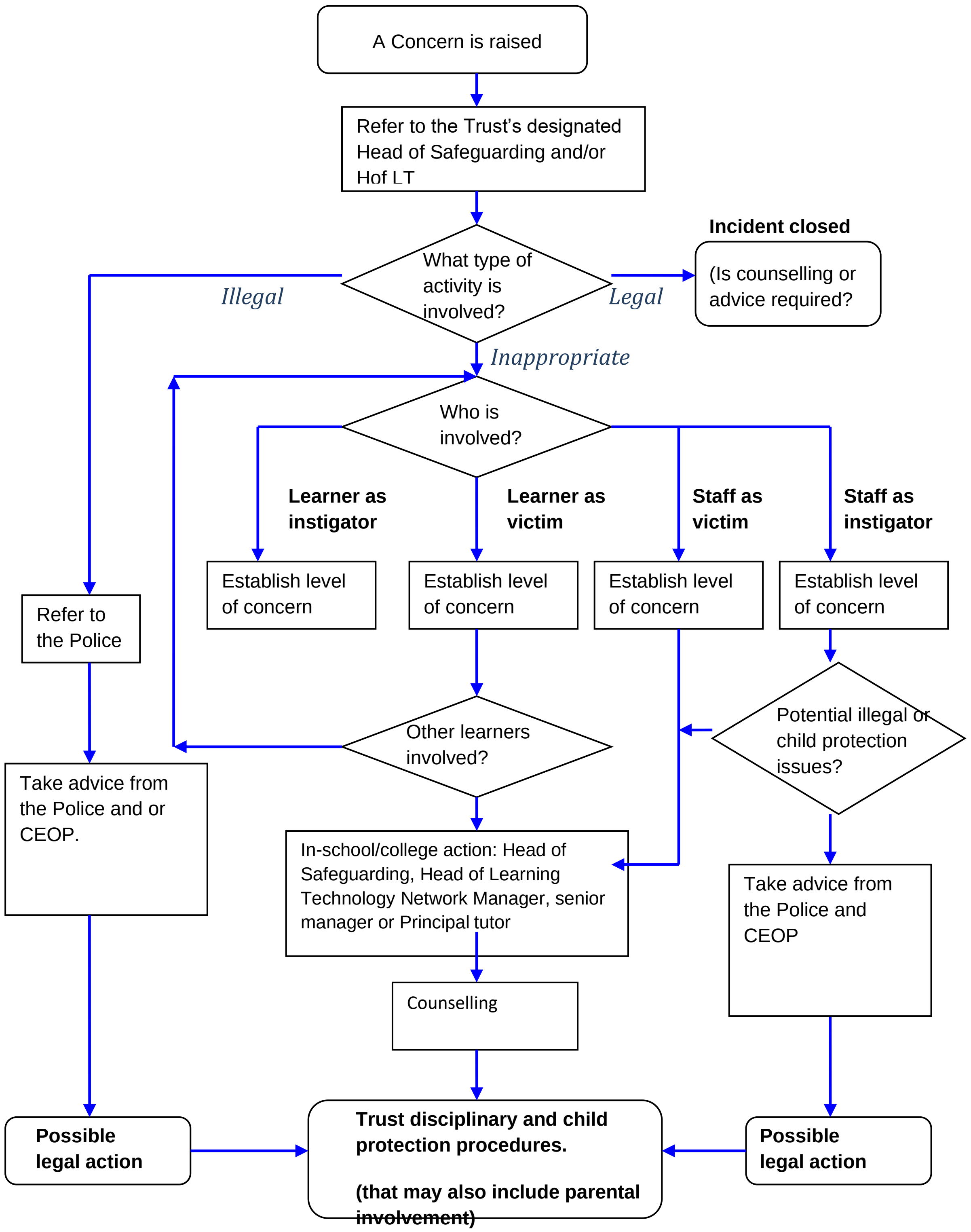
More serious incidents relating to e-safety should be reported to the Head of Safeguarding who will inform the Head of Learning Technology and Network Manager. The incident must be documented as quickly as possible and involve the Head of Safeguarding and other senior managers as appropriate. They will decide whether to involve the Police and Children's or Adult Social Care.

Serious incidents are likely to involve illegal material – the viewing, possessing, making or distribution of indecent images of children – serious stalking or harassment, or communication with children or vulnerable adults which amounts to abuse or 'grooming'.

9.3 Action

Discovery of indecent material or incriminating text or voicemail must always be reported to the Head of Safeguarding who will then inform the police. It is vital that the material is not downloaded, printed or sent by email because doing so may be an offence in itself. If at all possible, absolutely nothing should be done to the suspect computers or equipment, including turning them on or off. Ensure that everyone is kept away and nothing is touched and do not shut down the Network unless told to do so by the Police. The Police will be interested in obtaining 'best evidence' which will entail forensically copying hard drives or memory that may contain evidence of offences. A suspect computer or other equipment must not be viewed or used and advice must be sought from the local Police Hi-tech Crime Unit. Under no circumstances should an internal investigation be carried out. This could compromise evidence if a legal case should be the outcome.

9.4 Workflow


A Concern is raised
Refer to the Trust's designated Head of Safeguarding and/or Hof LT
What type of activity is involved?
Illegal
Legal
Incident closed
(Is counselling or advice required?
Inappropriate
Who is involved?
Learner as instigator
Learner as victim
Staff as victim
Staff as instigator
Establish level of concern
Establish level of concern
Establish level of concern
Establish level of concern
Refer to the Police
Other learners involved?
Potential illegal or child protection issues?
Take advice from the Police and or CEOP.
In-school/college action: Head of Safeguarding, Head of Learning Technology Network Manager, senior manager or Principal tutor
Take advice from the Police and CEOP
Counselling
Possible legal action
Trust disciplinary and child protection procedures.
(that may also include parental involvement)
Possible legal action

10. Further Action

A tutor may deal with a minor transgression of the rules, but the Head of Safeguarding will still be informed. A senior member of staff will deal with more serious complaints of Internet misuse. Any complaint about staff misuse must be referred to the Principal. Other situations could potentially be serious and a range of sanctions will be required, linked to the Trust's disciplinary policy. Potential safeguarding or illegal issues must be referred to the Trust's Head of Safeguarding and/or ILT Manager. Advice on dealing with illegal use could be discussed with the local Police Public Protection Unit to establish procedures for handling potentially illegal issues.

.

Measures for students within the Trust discipline policy include:

- Interview with senior member of staff;;
- Informing parents or carers;
- Removal of Internet or computer access for a period.

Disciplinary procedures will be initiated if staff do not follow the Trust E-safety policy.

11. Links to other related policies, procedures or documents (internal)

- Safeguarding Policy and procedures
- ICT Policy

12. Revision History

Listed below is a brief audit trail, detailing amendments made to this policy procedure in last 4 years

Page/para No.	Brief description of the change(s)	Change made by	Date
All	Minor amendments to reflect current management structure	Head of Safeguarding	April 2016
Para 7.3	Addition of reference to Twitter	Head of Safeguarding	April 2016
Para 7.2	Change to allow new recruits to keep existing social media friends and link to guide for staff safe usage.	Head of Safeguarding	April 2016
Annex A	Content removed and replaced with reference to different policy to avoid risk of synchronization error	Head of Safeguarding	April 2016
Para 11	Add links to other policies	Head of Safeguarding	April 2016
Throughout	Updated made throughout the document	Head of ILT Head of Technology	Oct 21

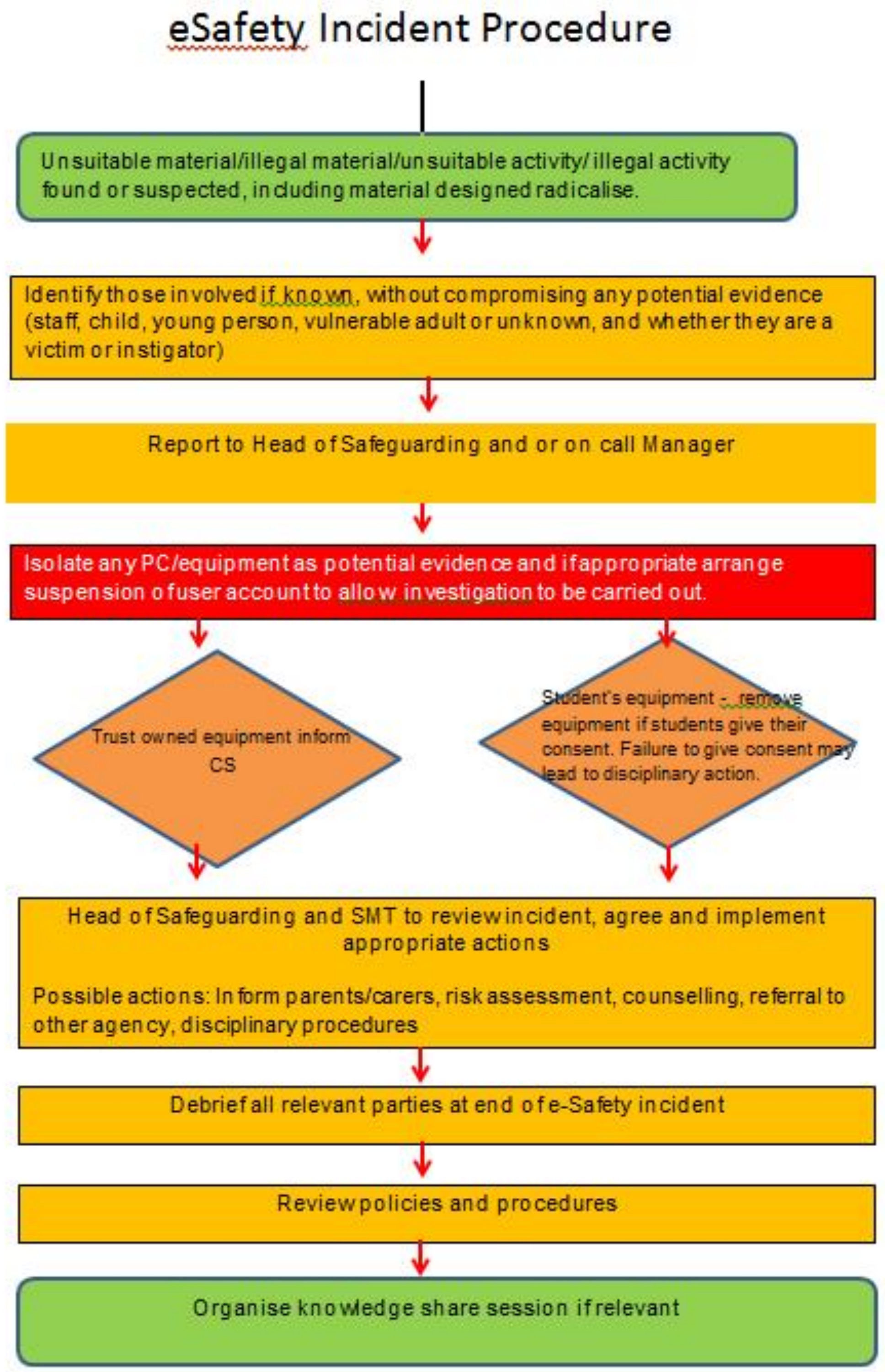
		Head of Safeguarding	
Para 7.1	Photography guidance clarified – particularly around swimming activities, following NSPCC/CPSU guidance	Head of Safeguarding	December 2023

IMPORTANT NOTES:

It is essential for those with designated responsibilities to familiarise themselves with the sources of information, referred to above.

Policy documents describe mandatory minimum standards and will be subject to audit and review. Line managers are required to ensure suitable and sufficient arrangements are in place to meet policy requirements, including the provision of information and instruction to staff.

Annex A



eSafety Incident Procedure

Unsuitable material/illegal material/unsuitable activity/ illegal activity found or suspected, including material designed radicalise.

Identify those involved if known, without compromising any potential evidence (staff, child, young person, vulnerable adult or unknown, and whether they are a victim or instigator)

Report to Head of Safeguarding and or on call Manager

Isolate any PC/equipment as potential evidence and if appropriate arrange suspension of user account to allow investigation to be carried out.

Trust owned equipment inform CS

Student's equipment - remove equipment if students give their consent. Failure to give consent may lead to disciplinary action.

Head of Safeguarding and SMT to review incident, agree and implement appropriate actions

Possible actions: Inform parents/carers, risk assessment, counselling, referral to other agency, disciplinary procedures

Debrief all relevant parties at end of e-Safety incident

Review policies and procedures

Organise knowledge share session if relevant

Student Acceptable Use Policy

The computers are provided at the School and College for use whilst you are a student. You must abide by the following rules in order to access the system.

Access to the Wifi is a privilege not a right, if you are identified as passing on the code to other staff or students this privilege may be removed. This is in place to prevent viruses on devices that have not been checked from being transferred to the network and also to ensure that students who should not have access to certain sites for legal and other reasons do not gain access to these.

You must not:

- Log on to the network with another user's account
- Reveal the Wifi code
- Use the computers to send offensive or unpleasant things to others
- Alter the settings of the computers or make changes which make them unusable by others
- Damage the equipment
- Install software from the Internet or from any other source.
- Hack into unauthorised areas of the network
- Access inappropriate web sites or trying to bypass the College filtering system
- Attempt to spread viruses via the network
- Using College computers for any form of illegal activity , including software and music piracy
- Obtain material in any format (including text, graphics, moving images, photographs, sound files etc.) which is illegal under the terms of the Obscene Publications Act, the Race relations Act or any other applicable UK legislation. Any such material downloaded accidentally must be deleted immediately.
- Print material unrelated to work. Users should be aware that printing is monitored and any private work can be charged for.

You need to be:

- Responsible for keeping your password confidential
- Aware that from time to time Computer Services may audit files, communications and Internet activity to ensure the safety of the system.
- Respect the work and ownership rights of people outside the Trust, as well as other students and staff. This includes abiding by copyright laws.
- Report to Computer Services, your Tutor or a member of staff any email containing material of a violent, dangerous, racist or inappropriate content.
- Follow the guidance in this document

Disciplinary action will be taken against those found to be in breach of the Acceptable Use Policy.

Signed or witnessed

(student): ____________________________

Date: ____________

Print Name

(student): ____________________________

Equality Impact Assessment (EIA) - Stage 1

Name of Policy / Function/Decision	E Safety Policy
Name of Assessor / Author /Lead	Jo Cox
Start Date	September 22
This EIA is being undertaken because it is:	A result of a policy revision
Screening	

Does the policy affect employees, students or other stakeholder groups? Could the impact be significant to that group of people?	Y
Is it a major policy with a significant effect on how our core business is delivered?	N
Does it involve a significant commitment of resources?	N
Does it relate to an area where there are known inequalities (e.g. gender pay gap, hate crime, accessibility of IT)	Y

If the answer to any of these questions is 'YES' then continue to complete Equality impact assessment. If you are unsure about the answer to any of these questions please contact EDI Co-ordinator or Head of Quality for further support.

Has the screening identified the policy as having relevance to the any of the following groups?

Age	N	Disability	N	Sexual Orientation	N
Race	N	Sex/Gender	N	Religion or Belief	N
Gender Reassignment	N	Pregnancy or Maternity	N	Marriage or civil partnership	N

Have we shown due regard for the 9 protected characteristics within the policy/procedure/decision?	Yes ☑ No ☐
Are all opportunities to promote equality taken within the policy/procedure/decision?	Yes ☑ No ☐

Have we stated how we will monitor the implementation and impact of this policy/decision?	Yes ☑ No □
Date of Screening	20th September 2022
Approval by EDI	Jo Cox
Refer Policy/Procedure to EDI Co-ordinator for further Stage 2 Assessment (if required)	Yes □ No ☑