Enquire Learning Trust E-safety Policy

Principles and purpose

New technologies have become integral to the lives of children and young people in today's society, both within and outside their school lives. The internet and other digital information technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and increase awareness of context to promote effective learning. Children and Young people should have an entitlement to safe internet access at all times.

The use of these new technologies can put young people at risk, some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to, loss of, sharing of personal information
- Risk of being subject to grooming by those with whom they make contact
- The sharing and distribution of personal images without their consent
- Inappropriate communication and contact with others
- Cyber-bullying
- Access to unsuitable video and internet games
- An inability to evaluate the quality, accuracy and relevance of e-information
- Plagiarism and copyright infringement
- Illegal downloading of music and video files
- Excessive use impacting on social and emotional development

Scope of the Policy

This policy applies to all employees and students wherever they may be, both at school or elsewhere such as at home when accessing systems which the school is responsible for.

Roles and Responsibilities

Pupils

It is the responsibility of the students to:

- Keep themselves safe when using ICT
- Report any instances of intentional or non-intentional breaches to this policy

Staff

It is the responsibility of all who work with children within school to:

- Comply with this policy
- Ensure that they understand the risks that the students face
- Promote e-safety at every opportunity with students
- In the event of a disclosure report it to the appropriate Senior Leadership Team in school

E-Safety Coordinator

It is the responsibility of the e-safety coordinator to:

- Develop an eSafety culture
- Act as a named point of contact on all eSafety issues for the Senior Leadership Teams
- Promote the eSafety vision to all stakeholders and supporting them in their understanding of the issues
- Ensure that eSafety is embedded within the continuing professional developments for staff and co-ordinate training as appropriate
- Ensure that eSafety is embedded across the curriculum and activities within the organisation as appropriate
- Ensure that eSafety is promoted to all stakeholders
- Support pastoral teams to decide on appropriate sanctions for pupils
- Monitor and report on eSafety issues to the management team, other agencies and the local authorities eSafety lead as appropriate
- Develop an understanding of the relevant legislation
- Liaise with the trust and other local bodies as appropriate
- Review and update eSafety policies and procedures on a regular basis

Principal/Head of School

The Principal/Head of School is responsible for:

- Ensuring appropriate arrangements are in place to comply with this policy
- Making sure all users are aware of this policy
- Ensuring that appropriate training is undertaken
- Ensuring that the technical infrastructure / network is as safe and secure as possible
- Updating the list of inappropriate websites which fall through the filtering software
- Supporting the investigation of eSafety incidents
- Applying sanctions to user accounts when necessary

Incident Management process in the event of an eSafety incident

Action to be taken when the breach is made by a member of staff:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policy the person who is made aware of this will report this to the designated lead for eSafety/safe guarding either INSERT NAMES	Member of Staff aware of the incident
The eSafety Co-ordinator will conduct an initial fact finding investigation which will ascertain who was involved, what has occurred. If appropriate the user will be restricted from access to the network	Principal/Head of School
The eSafety Co-ordinator will classify the incident appropriately (high or low severity) and enter details of the incident onto the member of staff's file	Principal/Head of School
The Principal/Head of School/line manager will have been informed and should be given the results of the initial fact finding investigation	Principal/Head of School
If appropriate discussions will take place between the Trust eSafety team and TCL to implement any necessary actions e.g. blocking a website	Principal/Head of School
The Principal/Head of School/line manager will discuss the concerns with the Trust Designated Officer (LADO) in order to discuss whether there is a need for a Strategy Meeting. During this discussion consideration will be given as to whether the police need to be involved. The Principal/Head of School/line manager will also discuss with Lauren Stones if the member of staff needs to be suspended or undertake different duties pending the completion of the enquiries.	Principal/Head of School
The Principal/Head of School/line manager will also discuss the incident with the eSafety lead in the Trust as consideration will need to be given to any further actions required.	Principal/Head of School/Line Manager
The strategy meeting process will be completed following the local Child Protection Appendix 4 Allegations Against Staff Protocol	
The designated lead will complete the agencies incident log and send a copy to the Trust's eSafety team	Principal/Head of School

Action to be taken when the breach is made by a young person:

	Person Responsible
Where there is concern that there has been a breach of the eSafety Policies the adult will make a decision whether to deal with it themselves by applying a sanction and logging it in SIMs or report it to the Senior Leadership Team. Guidance on severity and possible sanctions is in appendix 1	Member of Staff aware of the incident
The Senior Leadership Team will conduct an initial fact finding investigation who will ascertain who was involved, what sites have been accessed etc	Senior Leadership Team with support from the Principal/Head of School and ICT support
The Senior Leadership Team will classify the incident appropriately (high or low severity) and enter details of the incident into SIMs under E Safety / Abuse and make a decision about appropriate sanctions, with support from the Principal/head of School if necessary. They will also inform TCL to enable them to make changes to the computer system	Senior Leadership Team with support from Principal/Head of School and ICT support
If necessary, the Principal/Head of School will discuss the concerns with the manager of the local safeguarding team to establish if there are child protection concerns requiring a Section 47 Child Protection investigation. If this is required the local Safeguarding Team will conduct this investigation as required within the Child Protection Procedures	Principal/Head of School