Education Futures Trust

E-Safety and Acceptable Use Policy

Date of last review:	April 2023
Review date:	November 2027
Contact:	Chief Executive, Education Futures Trust

E-Safety and Acceptable Use Policy

This policy document sets out the Trust's aims, principles and strategies for E-Safety.

Everyone in the Trust, whether adult or child, has a duty to be aware of e- safety at all times, to know the required procedures and to act on them.

E-Safety is a safeguarding issue not an IT issue. Part of the Trust's vision is to prepare service users, especially children and young people, for the future and so the constant learning of new IT skills is essential as technology continues to develop. However, there are inherent dangers associated with connected technologies. It is therefore necessary that we take responsibility for e-safety and our key aim is to keep everyone safe.

E-Safety more commonly relates to the use of computers and mobile phones but does not exclude other hardware such as those which record images. The Trust has a responsibility to protect users from material of a pornographic, hateful or violent nature or which might encourage activities that are dangerous or illegal, age-inappropriate or biased. It alsoconcerns the protection of data held and used by the Trust and which might be saved on to a portable storage device such as a memory stick.

Safety measures in place

Staff laptops are encrypted. Whilst using Trust computers, all users will havetheir own log-ins and passwords to access the network and the internet. Passwords must not be shared.

Staff will be advised not to make their passwords too obvious and to avoid writing them down. All permanent staff and volunteers will sign a statement of intention relating to the use of the Trust's equipment and data.

Up-to-date anti-virus software is in place to provide further protection. However, no system is 100% safe.

A discussion around the use of IT and social media should be included within the induction period for both staff and volunteers.

Staff will be required to annually complete Local Authority approved Safeguarding training that covers use of IT and social media. Additional training will be provided in staff meetings so staff are aware of any current changes around the risks of IT and social media, for example, in relation to preventing extremism.

Children and young people

All children should be given guidance and will be made aware of their responsibilities if using Trust equipment.

Staff

The use of IT equipment should be appropriate to staff professional activities or the children's needs. Any personal, educational or medical data (electronic or paper copy) which is removed from the Trust's premises should be treated with extreme care. Electronic copies of sensitive information will be password protected, and paper copies securely stored and shredded after use.

Children should not be given access to any staff log-ins or passwords as this would allow them to view sensitive information. It is the responsibility of all staff to ensure

that material used for the purposes of Education Futures Trust is appropriate and does not infringe copyright laws.

All staff are responsible for monitoring children's activities and should report any concerns to their line manager. They should also seek advice if they are unclear of any of the issues referred to.

Staff should ensure that any equipment loaned by the Trust, whether on or off the Trust's premises, is not used to access or create inappropriate material and that any data stored on it is protected. They are alsoresponsible for making sure that any data brought into the Trust is free from viruses.

Images

A consent form must be filled out by parents/carers prior to the use of any images of children on the Trust's website, in the press or other media sources.

The Trust will only take and use images that are appropriate and are considered not to be open to misuse.

As the Trust provides the technology to take images, staff must not use their personal devices to take photographs/videos of service users.

If an image of a child is used, the child's name will not be published. If a name is published, no image will be used without specific consent. The image will not lead to the direct identification of individual pupils. Images will only be taken using Trust equipment or that which is approved by the Chief Executive before it is used.

For their own protection from allegations all staff are expected to have their personal mobile phones switched off when working directly withchildren.

All breaches of this policy will be taken seriously. Managers will monitor adherence to this policy and any issues relating to it. It is important that such issues are reported immediately (see Appendix 1). Where needed records may be shared with outside agencies.

Social Media

Staff should not cross professional boundaries in their use of social media. There should not be contact with service users through personal accounts. Where there are original personal relationships prior to involvement in EFT activities, then a conflict of interest form must be completed and a discussion with a line manager should identify appropriate steps to retain the integrity of the service and the organisation.

Volunteers should declare any links to other service users at the start of a volunteering period and be advised on how to maintain the integrity of their role and the organisation.

Further guidance

UKCICS:
https://www.gov.uk/government/groups/uk-council-for-child-internet- safety-ukccis

NSPCC:
Online safety resources for schools and organisations | NSPCC Learning

Protecting children from online abuse | NSPCC Learning

The Byron Report
Ten years since the Byron Review (nspcc.org.uk)

E-Safety representatives:

Trustee:	Allison Baines
Chief Executive	Carole Dixon
Designated Person:	Carole Dixon
Managers:	Shar Brown.
	Marie Burgess

Education Futures Trust

Appendix 1

Where it is deemed necessary to preserve evidence of a serious breach of e-safety:

1. Do not touch the computer or device in question. Any contact with the hardware may contaminate the evidence trail.
2. Contact the Chief Executive stating clearly that you have a high priority e-safety incident and that you need to preserve an evidence trail. Note the advice given to you.
3. If the event involves a child, how you respond will be dictated by the event and its origin. Contact with the parents and carers would be appropriate. Keep records of conversations. However, if the event occurred within the family and has been the subject of a disclosure, speak to the Designated Safeguarding Lead about a referral to the LSCB.

Where it is deemed necessary to contact external agencies, keep clear records of all conversations.