E safety policy

E safety policy

1. Purpose and Scope

This e-Safety policy recognises the commitment of CareTrade to e-Safety and acknowledges its part in the charities' overall Safeguarding policies and procedures. It shows our commitment to meeting the requirement to keep learners safe when using technology.

We believe the whole community can benefit from the opportunities provided by the Internet and other technologies used in everyday life. The e-Safety policy supports this by identifying the risks and the mitigating actions we are taking to avoid them. It shows our commitment to developing a set of safe and responsible behaviours that will enable us to reduce the risks whilst continuing to benefit from the opportunities. It ensures that all staff, volunteers and service users are aware that unlawful or unsafe behaviour is unacceptable and that, where necessary disciplinary or legal action will be taken.

Other policies to refer to:

- Preventing Extremism and Radicalisation Policy
- Adult at Risk Safeguarding and Protection Policy and Procedures
- Child at Risk Safeguarding and Protection Policy and Procedures
- Data Protection Policy

As part of our commitment to e-Safety we also recognize our obligation to implement a range of security measures to protect the charities network and facilities from attack, compromise and inappropriate use and to protect charity data and other information assets from loss or inappropriate use.

This policy applies to our entire community including all staff employed directly or indirectly by the charity, visitors and all learners.

Senior staff and the Charity Trustees will ensure that any relevant or new legislation that may impact upon the provision for e-Safety within the charity will be reflected within this policy. Senior staff will ensure all members of staff are aware of the contents of the charities e-Safety policy and the use of any new technology within charity.

2. Guidance for Staff and volunteers

2.1 Communication with Young People (including the Use of Technology)

Communication between staff and students by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

Staff should not share any personal information with a young person. They should not request, or respond to, any personal information from the young person, other than that which might be appropriate as part of their professional role.

Staff should ensure that all communications are transparent and open to scrutiny. Staff should also be circumspect in their communications with young people so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as grooming. They should not give their personal contact details to young people including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management.

E-mail or text communications between an adult and a young person outside agreed protocols may lead to disciplinary and/or criminal investigations. This also includes communications through internet based web sites such as Facebook.

This means that staff and volunteers should:

- **Not** give their personal contact details to college learners, including their personal mobile telephone number and details of any blogs/vlogs or personal websites.
- **only use equipment** e.g. mobile phones, **provided by organisation to communicate with learners** (where a young person is under 18 parental permission must be sort also)
- **only make contact with learners for professional reasons** and in accordance with any organisation policy
- **Be aware of individual students preferred means of communication (email, text or call) and also be aware of how a student may communicate with staff in a crisis situation or at risk of harm.** This will be documented in each students individual file notes.
- **Not** use internet or web-based communication channels to send personal messages to college learners.
- Ensure that if a social networking site is used, details **are not** shared with students and privacy settings are set at maximum.

Access to Inappropriate Images and Internet Usage

There are no circumstances that will justify adults possessing indecent images of young adults. Adults who access and possess links to such websites will be viewed as a significant and potential threat to children/young adults. Accessing, making and storing indecent images of young adults on the internet is illegal. This will lead to criminal investigation and the individual being barred from working with children and young adults, if proven.

- Adults must not use equipment belonging to their organization to access adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with young adults and will result in disciplinary action and possible criminal investigation.

- **Adults should ensure that young adults are not exposed to any inappropriate images or web links.** Organizations and adults need to ensure that internet equipment used by the students have the appropriate controls with regards to access. **E.g. personal passwords should be kept confidential.**

- Where indecent images of children or other unsuitable material are found, the police and Local Authority Designated Officer (LADO) should be immediately informed. Staff should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.

- **Staff should never allow a student to use their personal phone and only allow a student to use their phone in exceptional circumstances and never unsupervised.**

Who is involved in the process?

E-Safety is the responsibility of the whole charity and everyone has their part to play in ensuring all members of the charity are able to benefit from the opportunities that technology provides for learning and teaching. The CEO on behalf of the Trustees has ultimate responsibility for the e-Safety for the charity and should:

- Identify a person (the e-Safety lead) to take day to day responsibility for eSafety; provide them with training; monitor and support them in their work. The E- Safety Lead for CareTrade is the Employment Opportunities Manager (See Staff responsibility sheet for more information)
- Ensure adequate technical support is in place to maintain a secure ICT system -Premier Choice currently provide us with all technical support.
- Ensure policies and procedures are in place to ensure the integrity of the charities information and data assets.
- Ensure liaison with the Trustees
- Develop and promote an e-Safety culture within the charity
- Policy and that new staff have e-Safety included as part of their induction procedures
- Make appropriate resources, training and support available to all members of the charity to ensure they are able to carry out their roles effectively with regard to e-Safety
- Receive and regularly review e-Safety incident logs; ensure that the correct procedures are followed should an e-Safety incident occur in charity and review incidents to see if further action is required. We have an e safety incident log that can be found in our Policy File.

Responsibilities of the e-Safety Lead

- Promote an awareness and commitment to e-Safety throughout the charity
- Be the first point of contact in charity on all e-Safety matters
- Take day to day responsibility for e-Safety within the charity
- Lead the charity and/or liaise with technical staff on e-Safety issues

- Create and maintain e-Safety policies and procedures
- Develop an understanding of current e-Safety issues, guidance and appropriate legislation
- Ensure delivery of an appropriate level of training in e-Safety issues
- Ensure that e-Safety education is embedded across all curriculum
- Ensure that e-Safety is promoted to parents and carers
- Ensure that any person who is not a member of charity staff who makes use of ICT equipment in any context, is made aware of the ICT Acceptable Use Policy
- Liaise with the Local Authority, the Local Safeguarding Board and other relevant agencies as appropriate
- Monitor and report on e-Safety issues to SLT and the Safeguarding Lead as appropriate
- Ensure that staff and students know the procedure to follow should they encounter any material or communication that makes them feel uncomfortable and how to report an e-Safety incident in the e –safety incident log
- Ensure an e-Safety incident log is kept up-to-date
- Ensure that Good Practice Guides for e-Safety are displayed in classrooms and office
- To promote the positive use of modern technologies and the internet
- To ensure that the charity e-Safety policy and Acceptable Use Policies are reviewed at prearranged time intervals.

Responsibilities of all Staff

- Read, understand and help promote the charities e-Safety policies and guidance
- Read, understand and adhere to the AUP
- Take responsibility for ensuring the safety of sensitive data and information.
- Develop and maintain an awareness of current e-Safety issues, legislation and guidance relevant to their work
- Maintain a professional level of conduct in their personal use of technology at all times • Ensure that all digital communication with learners is on a professional level and only through charity based systems, NEVER through personal email, text, mobile phone social network or other online medium
- Embed e-Safety messages in learning activities where appropriate
- Supervise students carefully when engaged in learning activities involving technology
- Ensure that students are told what to do should they encounter any material or receive a communication which makes them feel uncomfortable
- Report all e-Safety incidents which occur in the appropriate log and/or to their line manager
- Respect, and share with students the feelings, rights, values and intellectual property of others in their use of technology in a learning environment and at home.

Additional Responsibilities of ICT Staff /E safety Lead

Please note that currently we have an external organisation that support us in providing a safe technical infrastructure to support learning and teaching.

- Ensure appropriate technical steps are in place to safeguard the security of the charity ICT system, sensitive data and information. Review these regularly to ensure they are up to date
- Ensure that provision exists for misuse detection and malicious attack
- At the request of the SLT conduct occasional checks on files, folders, email and other digital content to ensure that the Acceptable Use Policy is being followed
- Report any e-Safety-related issues that come to their attention to the e-Safety lead and/or SLT
- Ensure that procedures are in place for new starters and leavers to be correctly added to and removed from all relevant electronic systems, including password management
- Ensure that suitable access arrangements are in place for any external users of the charities ICT equipment
- Liaise with the Local Authority and others on e-Safety issues
- Document all technical procedures and review them for accuracy at appropriate intervals
- Ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster

Responsibilities of Parents and Carers

- Help and support the charity in promoting e-Safety
- Discuss e-Safety concerns with students, show an interest in how they are using technology, and encourage them to behave safely and responsibly when using technology
- Consult with the charity if they have any concerns about a students use of technology

Responsibilities of Trustee Body

- Read, understand, contribute to and help promote the charities e-Safety policies and guidance as part of the charities overarching Safeguarding procedures
- Support the work of the charity in promoting and ensuring safe and responsible use of technology in and out of educational environment, including encouraging parents to become engaged in e-Safety awareness
- To have an overview of how the charity IT infrastructure provides safe access to the internet and the steps the college takes to protect personal and sensitive data

The Process Learning and Teaching

We believe that the key to developing safe and responsible behaviours online for everyone within the charity lies in effective education. We know that the Internet and other technologies are embedded in our young person's lives, not just in a learning environment but outside as well, and we believe we have a duty to help prepare our students to benefit safely from the opportunities that these present. We will deliver a planned and progressive scheme of work to teach e-Safety knowledge and

understanding and to ensure that learners have a growing understanding of how to manage the risks involved in online activity. We believe that learning about e-Safety should be embedded across the curriculum. We will discuss, remind or raise relevant e-Safety messages with students routinely wherever suitable opportunities arise. This includes the need to protect personal information and to consider the consequences their actions may have on others. Staff will model safe and responsible behaviour in their own use of technology during classroom sessions/1; 1 sessions. Students will be made aware of where to seek advice or help if they experience problems when using the internet and related technologies.

Access to charity systems

The charity decides which users should and should not have Internet access, the appropriate level of access and the level of supervision they should receive. There are robust systems in place for managing network accounts and passwords, including safeguarding administrator passwords. Suitable arrangements are in place for visitors who may be granted a temporary log in. Staff are given appropriate guidance on managing access to laptops which are used both at home and college and in creating secure passwords. Access to personal, private or sensitive information and data is restricted to authorized users only, with proper procedures being followed for authorizing and protecting login and password information. Remote access to systems is covered by specific agreements and is never allowed to unauthorized third party users.

Using the Internet

We provide the internet to

- Support curriculum development in all subjects
- Support the professional work of staff as an essential professional tool
- Enhance the charities management information and business administration systems
- Enable electronic communication and the exchange of curriculum and administration data with the LA, the examination boards and others Users are made aware that they must take responsibility for their use of, and their behaviour whilst using the IT systems or a provided laptop or device and that such activity can be monitored and checked.

Dealing with e-Safety incidents

- All e-Safety incidents are recorded in the incident log which is regularly reviewed. In situations where a member of staff is made aware of a serious e-Safety incident, concerning students or staff, they will inform the e-Safety Lead or their line manager who will then respond in the most appropriate manner
- Instances of cyberbullying will be taken very seriously by the college and dealt with using the charities anti-bullying procedures.
- Charity recognises that staff as well as students may be victims and will take appropriate action in either situation, including instigating restorative practices to support the victim. Incidents which create a risk to the security of the network, or create an information security risk, will be referred to the e-Safety Lead and technical support and appropriate advice sought and action taken to minimize the

risk and prevent further instances occurring, including reviewing any policies, procedures or guidance. If the action breaches policy then appropriate sanctions will be applied.

- The charity will decide if parents/carers need to be informed if there is a risk that data has been lost.
- CareTrade reserves the right to monitor equipment on their premises and to search any technology equipment, including personal equipment with permission, when a breach of this policy is suspected.

Dealing with an Adult Protection issue arising from the use of technology

If an incident occurs which raises concerns about Adult Protection or the discovery of indecent images on the computer, then the procedures outlined in the Safeguarding Procedures and Guidance will be followed.

There may be occasions when the police must be contacted. Early contact will be made to establish the legal position and discuss strategies. The following activities constitute behaviour which we would always consider unacceptable (and possible illegal):

- accessing inappropriate or illegal content deliberately
- deliberately accessing downloading and disseminating any material deemed offensive, obscene, defamatory, racist, homophobic or violent
- continuing to send or post material regarded as harassment, or of a bullying nature after being warned
- staff using digital communications to communicate with learners in an inappropriate manner (for instance, using personal email accounts, personal mobile phones, or inappropriate communication via social networking sites)

The following activities are likely to result in disciplinary action

- any online activity by a member of the charity which is likely to adversely impact on the reputation of the charity
- accessing inappropriate or illegal content accidentally and failing to report this
- inappropriate use of personal technologies (e.g. mobile phones) at work or in lessons
- sharing files which are not legitimately obtained e.g. music files from a file sharing site
- using charity or personal equipment to send a message, or create content, that is offensive or bullying in nature or could bring the college into disrepute
- attempting to circumvent charity filtering, monitoring or other security systems
- circulation of commercial, advertising or ‘chain’ emails or messages
- revealing the personal information (including digital images, videos and text) of others by electronic means (e.g. sending of messages, creating online content) without permission
- using online content in such a way as to infringe copyright or which fails to acknowledge ownership (including plagiarizing of online content)
- transferring sensitive data insecurely or infringing the conditions of the Data Protection Act, revised 1988