



Online Safety Policy

1. Introduction

1.1 Aims

1. Have robust processes in place to ensure the online safety of learners/participants/ clients, staff, volunteers, and trustees.
2. Deliver an effective approach to online safety, which empowers us to protect and educate the whole CareTrade community in its use of technology.
3. Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

1.2 Purpose & Background

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

We believe the whole community can benefit from the opportunities provided by the Internet and other technologies used in everyday life.

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/ participants/clients.

1.3 Link to Vision and Beliefs

CareTrade's belief is "*... that employment is the biggest single factor that will transform the life of an autistic person...*"

CareTrade's vision for the future is "*A world that embraces neurodiversity in the workplace and all autistic people lead a purposeful, working, life*"

This can only be attained if young people and adults are educated how to keep themselves safe online whilst in and out of the workplace.

1.4 Link to CareTrade's other Policies and Procedures

CareTrade's ICT Acceptable Use policy also supports this policy as it ensures all staff, learners, participants, and clients complete an ICT user agreement. The user agreement clearly explains what CareTrade technology can and cannot be used for. Completed forms are then saved securely in the correct folder on SharePoint:

- CareTrade staff in the Leadership folder
- TAP learners in the TAP folder
- Project participants or ATW clients in the Development folder

The ICT user agreement supports the e-safety policy 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, learners, participants, and clients 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:

- Data Protection/ GDPR Policy
- Behaviour and Conduct Policy
- Health and Safety Policy
- Wellbeing Policy

2. Roles and Responsibilities

2.1 The Trustee board

The trustee board has overall responsibility for monitoring this policy and holding the headteacher to account for its implementation.

The trustee board will co-ordinate regular meetings with appropriate staff to discuss online safety and monitor online safety logs as provided by the designated safeguarding lead (DSL).

All trustees will:

- Ensure that they have read and understand this policy.
- Agree and adhere to the terms on acceptable use of the CareTrade's ICT systems and the internet (appendix 3)

2.2 The Head of Education & Learning

The Head of Education & Learning **Mark Finch** is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout CareTrade.

2.3 The Designated Safeguarding Leads

Details of the CareTrade's DSL's are set out in our Safeguarding & Prevent policy.

The following DSLs **Mark Finch, Jemma Dear, Judith Kerem and Aga Keeling** takes lead responsibility for online safety within their team/ project, in particular:

- Supporting the Head Of E&L in ensuring that staff understand this policy and that it is being implemented consistently throughout CareTrade.
- Working with the Head of E&L, ICT manager and other staff, as necessary, to address any online safety issues or incidents.
- Ensuring the online safety is embedded into the curriculum and covered in induction for learners or participants.
- Ensuring that any online safety incidents are logged on Smoothwall and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the CareTrade behaviour policy.
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary

2.3 The ICT Manager

The ICT manager **Karen Edwards** is responsible for:

Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep learners/participants/clients safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material.

Ensuring that the CareTrade's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly.

Working with the above DSL's by conducting a full security check and monitoring the CareTrade's ICT systems on a monthly basis

Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files

2.4 All staff and volunteers

All staff, including contractors and agency staff, and volunteers are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the CareTrade's ICT systems and the internet and ensuring that learners/participants/clients follow the CareTrade's terms on acceptable use.
- Working with the DSL to ensure that any online safety incidents are logged on Smoothwall and dealt with appropriately in line with this policy.
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the CareTrade's behaviour policy.

2.5 Visitors and members of the CareTrade community

Visitors and members of the community who use the CareTrade's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it. If appropriate, they will be expected to agree to the terms on acceptable use.

3. Guidance for Staff and Volunteers

Communication with learners/participants/clients (including the Use of Technology)

- **Communication between staff and learners/participants/clients 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, webcams, websites, virtual meetings on platforms such as Zoom or Teams and blogs.
- **Staff should only contact learners/participants/clients within their working hours of 9am – 5.30pm.** Any communication outside of these hours would need to be agreed with their line manager before.
- **Staff should not share any personal information with a learner/participant/client.** They should not request, or respond to, any personal information from the learner/participant/client, 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 a learner/participant/client 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 a learner/participant/client including e-mail, home or mobile telephone numbers.
- **Staff should always follow the Online Learning Safeguarding Guidelines** when delivering a session online.
- **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, Instagram or Twitter.

This means that staff and volunteers should:

- **Not** give their personal contact details to learners/participants/clients 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/participants/clients.
- **Only contact learners/participants/clients for professional reasons** and in accordance with any organisation policy
- **Be aware of individual learners/participants/clients preferred means of communication** (email, text or call) and also be aware of how a learner may communicate with staff in a crisis situation or at risk of harm. This will be documented in each learner's individual file notes.
- **Not to use** own personal internet or web-based communication channels to send personal messages to learners/participants/clients.
- **Staff to ensure** that if a social networking site is used, details are not shared with learners/participants/clients and privacy settings are set at maximum.

4. Cyber-bullying

4.1 Definition

Cyber-bullying takes place online, such as through social networking sites, messaging apps or gaming sites. Like other forms of bullying, it is the repetitive, intentional harming of one person or group by another person or group, where the relationship involves an imbalance of power.

4.2 Preventing and addressing cyber-bullying.

To help prevent cyber-bullying, we will ensure that learners/participants/clients understand what it is and what to do if they become aware of it happening to them or others. We will ensure that learners/participants/clients know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim.

CareTrade will actively discuss cyber-bullying with learners/participants/clients, explaining the reasons why it occurs, the forms it may take and what the consequences can be. CareTrade staff will discuss cyber-bullying with their learners/participants.

CareTrade staff are also encouraged to find opportunities to use aspects of the curriculum to cover cyber-bullying. This includes personal, social, health and economic (PSHE) education, and other subjects where appropriate.

All staff and volunteers (where appropriate) receive training on cyber-bullying, its impact and ways to support learners/participants/clients, as part of safeguarding training.

In relation to a specific incident of cyber-bullying, CareTrade will follow the processes set out in the school behaviour policy. Where illegal, inappropriate, or harmful material has been spread among pupils, the school will use all reasonable endeavours to ensure the incident is contained.

The DSL will consider whether the incident should be reported to the police if it involves illegal material and will work with external services if it is deemed necessary to do so.

4.3 Examining CareTrade electronic devices.

CareTrade staff will carry out termly checks on the electronic devices, including mobile phones, that is access by learners/participants/clients.

When carrying out a termly check staff will check the following:

- Search history
- Files including images saved on the device.

If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL or other member of the senior leadership team to decide whether they should:

- Delete that material, or
- Retain it as evidence (of a criminal offence or a breach of CareTrade discipline), and/or
- Report it to the police

5. Acceptable use of the internet at CareTrade

All learners/participants/clients, staff, and volunteers are expected to sign an agreement regarding the acceptable use of the CareTrade's ICT systems and the internet.

Visitors will be expected to read and agree to the CareTrade's terms on acceptable use if relevant.

Use of the CareTrade's internet must be for project purposes only, or for the purpose of fulfilling the duties of an individual's role.

We will monitor the websites visited by learners/participants/clients, staff, volunteers, and visitors (where relevant) to ensure they comply with the above.

6. How will CareTrade respond to issue of misuse.

Where a learner/participant/client misuses the CareTrade's ICT systems or internet, we will follow the procedures set out in our policies on ICT and internet acceptable use, action taken will depend on the individual circumstances, nature, and seriousness of the specific incident, and will be proportionate.

Where a staff member misuses the CareTrade's ICT systems or the internet or misuses a personal device where the action constitutes misconduct, the matter will be dealt with in accordance with the staff code of conduct. The action taken will depend on the individual circumstances, nature, and seriousness of the specific incident.

The CareTrade will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

7. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues including cyber-bullying and the risks of online radicalisation.

All staff members will receive refresher training at least once each academic year as part of safeguarding training, as well as relevant updates as required (for example through emails, e-bulletins, and staff meetings).

The DSL will undertake safeguarding training, which will include online safety, at least every 2 years. They will also update their knowledge and skills on the subject of online safety at regular intervals, and at least annually.

Trustees will receive training on safe internet use and online safeguarding issues as part of their safeguarding training.

Volunteers will receive appropriate training and updates, if applicable.

More information about safeguarding training is set out in our Safeguarding and Prevent Policy.