CELT

E-safety
&
ICT Policy and Procedures

Contents

Document Revision

Date	Staff Involved
Policy written by:	Neil Harris
Policy reviewed by:	Grace Durighello, Greg Nelson, Mike Burden, (Designated Safeguarding Staff)
Policy approved by:	Greg Nelson
Policy publication date:	December 2018
Policy amended:	
Next policy review date:	December 2019

DESIGNATED SAFEGUARDING STAFF

Greg Nelson (Principal), Responsible for IT and ICT/E-Safety Policy and Procedures

greg@celt.co.uk +44(0) 2920 339290

Mike Burden (Director of Studies), Designated Safeguarding Person

mike@celt.co.uk +44(0) 2920 339290

Neil Harris (Academic Projects Development Manager), Assistant Designated Safeguarding Person

neil@celt.co.uk +44(0) 2920 339290

Grace Durighello (Academic Director)

grace@celt.co.uk +44(0) 2920 339290

This policy was last updated in December 2018. The next update is due in December 2019.

1. Context

Founded in 1989, CELT offers courses for adults at its adult centre in Salisbury Road, Cardiff and courses for under 18s (aged 13-17) in its dedicated junior centre in North Road. The school also accepts 17-year-old learners on its adult courses in Salisbury Road, subject to receipt of the necessary parental consent forms. Adult courses run year-round; junior courses run year-round for closed groups and with continuous enrolment in open classes in July and August on the under 18 Holiday Language Course.

CELT recognises that the use of internet technologies and communication devices are now seen as a vital life skill and that the use of these can help to enhance communication and the sharing of information. However, CELT is also aware that the use of these technologies has the potential to challenge the definitions and boundaries of learning and teaching.

Current internet technologies and electronic communication devices used by students and staff inside of CELT may include, and are not limited to:

- Internet websites
- Instant Messaging (IM)
- Social media & networking sites (such as Facebook, Instagram, Snapchat and Twitter)
- Email
- Video broadcasting sites (such as YouTube)
- Smart phones with email and web applications
- Tablets and mobile phones with digital cameras
- Laptops and desktop PC's

CELT recognises that all of these have the potential to help improve standards of learning and teaching and contribute to pastoral care but may equally present challenges to both students and staff in terms of keeping safe. The main areas of risk for CELT can be summarised as follows:

- exposure to inappropriate or illegal content, including online pornography, extremism, ignoring age ratings in games (exposure to violence associated with often racist language)
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites
- identity theft or invasion of privacy
- hate sites
- grooming
- cyber-bullying in all forms
- receiving sexually explicit images or messages (sexting)
- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online - internet or gaming)
- copyright (little care or consideration for intellectual property and ownership – such as music and film)

2. Key Terminology

Child Protection
This is part of safeguarding and promoting welfare. This refers to the activity that is undertaken to protect specific children who are suffering, or likely to suffer significant harm.

Children and under 18s
The Children Act 1989 states the legal definition of a 'child' as a 'person under the age of 18. The terms 'child' and 'under 18' are used interchangeably in this policy.

Cyber-bullying
This refers to bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers and tablets, as well as communication tools including social media sites, text messages, chat and websites.

Examples of cyberbullying include mean text messages or emails, rumours sent by texts, email or social networking sites, embarrassing pictures or videos posted on websites and the creation of fake profiles.

Designated Safeguarding Person (DSP)
This person takes overall responsibility for safeguarding and leading the team of Designated Safeguarding Staff (DSS).

Designated Safeguarding Staff (DSS)
CELT has a number of DSS to help lead and co-ordinate safeguarding practice for children and vulnerable adults.

E-safety
The safe and responsible use of internet technology and other electronic communications. Information and Communications Technology (ICT) ICT (information and communications technology - or technologies) is an umbrella term that includes any communication device or application, encompassing: radio, television, cellular phones, computer and network hardware and software, satellite systems and so on.

Stakeholders
All students, staff, volunteers, visitors and contractors who attend, visit or provide services for CELT.

Safeguarding
Safeguarding and promoting the welfare of children is:

- protecting children from harm
- protecting children from that which is not in their best interests
- preventing the impairment of children's health and safety

Social media
Websites and applications that enable users to create and share content or to participate in social networking.

Social networking
The use of websites and other internet services to communicate with other people and make friends.

Vulnerable adults
A person can be considered to be 'vulnerable' if they are "in need of community care services by reason of mental or other disability, age or illness; and is or may be unable to take care of him or herself, or unable to protect him or herself against significant harm or exploitation" (Lord Chancellor's Department, 1997). This definition of adult covers all people over 18 years of age.

3. Policy Statement

This E-safety and ICT Policy relates to all stakeholders CELT (including students, staff, volunteers, visitors and contractors) who have access to, and are users of internet technologies and electronic communications both in and out of CELT venues where actions relate to CELT activities, or the use of CELT ICT systems.

Safety and wellbeing is the collective and individual responsibility of all its stakeholders.

CELT aims to ensure that regardless of age, gender, race, ethnicity, religion or beliefs, sexual orientation, socio-economic background, all stakeholders have a positive and safe learning, teaching and working experience.

The purpose of this policy is as follows:

- To set out the key principles expected of all members of the school community at CELT with respect to the use of ICT-based technologies.
- To safeguard and protect all students (under 18s & adults), homestays and staff of CELT
- To assist school staff working with students to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice.
- To set clear expectations of behaviour and/or codes of practice relevant to responsible use of the internet for educational, personal or recreational use.
- To have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies.
- To ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.
- To minimise the risk of misplaced or malicious allegations made against adults who work with students.

4. Roles and Responsibilities

- **The Principal**
- Overall responsibility for e-Safety provision
- Overall responsibility for data and data security
- To ensure the school uses an approved filtered Internet service

As the Principal is also responsible for IT support, his responsibilities also extend to:

- Reporting any e-safety issues that arise to the DSP
- Ensuring that staff users may only access the school's networks through an authorised and properly enforced password protection policy.
- Ensuring that provision exists for misuse detection and malicious attack e.g. keeping virus protection up to date.

- Ensuring that appropriate back up procedures exist so that critical information and systems can be recovered in the event of a disaster

Designated Safeguarding Person and Assistant Designated Safeguarding Person

- Promotes awareness of and commitment to e-safeguarding throughout the school
- Ensures all staff are aware of the procedures that need to be followed in the event of an e-Safety incident
- Ensures that a safeguarding record is made in the case of an incident involving a student under 18
- Is regularly updated on e-safety issues and legislation and aware of the potential for serious child protection issues to arise from:
  - Sharing of personal data
  - Access to illegal/inappropriate materials
  - Inappropriate online contact with adults/strangers
  - Potential or actual incidents of grooming
  - Cyber-bullying and use of social media
- To oversee the delivery of the e-safety element of the induction for under 18s (this is covered in their absence by either the Academic Director or the Principal)

Teachers

- To supervise and guide students under 18 carefully when engaged in learning activities involving online technology.

All staff

- To read, understand and help promote the school's e-Safety policies and guidance.
- To be aware of e-Safety issues related to the use of mobile phones and other hand held devices and to monitor their use and implement the relevant school policies.
- To report any suspected misuse to the Principal.
- To model safe, responsible and professional behaviour in their own use of technology.
- To ensure that any digital communications with students should be on a professional level and only through school based systems, never through personal email, texts etc.

Students

- To understand the importance of reporting abuse, misuse or access to inappropriate materials, particularly in relation to students under 18.
- To know and understand the school's policy on cyber-bullying
- To understand the importance of adopting good e-Safety practice when using digital technologies particularly in relation to under 18s

Homestays

- To understand the importance of reporting abuse, misuse or access to inappropriate materials, particularly in relation to under 18s

Communication:

- Policy to be posted on the school website and available with the school's Safeguarding policy in the DSP's and Owner Directors' offices: summary in poster form on school noticeboards
- All students under 18 to have an IT safe use induction as part of their school induction
- Staff and homestay responsibilities summarised in staff code of conduct for under 18-year olds

5. Code of Conduct

This code of conduct:

- Assists stakeholders in working safely and responsibly and monitoring their own standards and practice.
- Sets clear expectations of behaviour and codes of practice relevant to e-safety and use of ICT
- Supports stakeholders by giving a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken.

6. E-Safety and students under 18

While mobile phones and access to the Internet offer students convenient and rapid means of contact with their friends and family back home, and therefore have a valuable welfare role, they also provide opportunities for abuse and inappropriate behaviour. In particular, there are risks to young people through cyberbullying (possibly by their peers), exposure to radical/extremist views, grooming by adult sexual predators, and downloading and or sharing of illegal, inappropriate or copyrighted materials and possibly computer viruses. The school has therefore established the following guidelines:

- Staff should not give out their personal mobile number, email address, Facebook contact details to students, especially those under 18. The exception to this would be homestays providing emergency contact details to students staying with them, especially under 18s.

- Inappropriate access to websites should be reported to the Principal. Inappropriate websites include pornographic and extremist sites, excessively violent videos and games, and some age inappropriate social networks and chat rooms. Most inappropriate sites are in fact blocked on the school network but may be accessed by students in a home setting. Therefore, all staff are asked to be vigilant regarding use of the internet by under 18 year olds, and if there are concerns about content, excessive use or possible grooming or abuse, they should be reported and/or action taken to remove access.

- All students are made aware of the school's IT policies at induction and these are displayed prominently in the school and in particular in the computer rooms. E-safety is covered as part of their induction. In particular, students will:

    - have to sign an e-safety user contract prior to using our systems
    - understand acceptable behaviour when using an online environment/email, i.e. be polite, no bad or abusive language or other inappropriate behaviour such as sexting; keeping personal information private
    - understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - understand why they must not post pictures or videos of others without their permission;
    - know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the internet and related technologies

7. Managing the ICT infrastructure

Email

Students and staff must immediately tell a designated member of staff if they receive an offensive email. Staff will only use official work-provided email accounts to communicate with other stakeholders (including students, parents, carers and third parties).

Emails must not be used to forward inappropriate messages or content to any individual.

Internet access, security (virus protection) and filtering

This school:

- Uses a filtering system which blocks at source by the ISP sites that fall into categories such as pornography, race hatred and other forms of extremism, gaming, sites of an illegal nature, etc.
- Ensures network is healthy through use of anti-virus software and a firewall
- Is vigilant in its supervision of under 18s use at all times, as far as is reasonable;
- Is vigilant when conducting image searches with under 18s e.g. Google image search;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Principal.
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse.
- Provides advice and information on reporting offensive materials, abuse/ bullying etc

Network management (user access, backup)

- Storage of all data within the school will conform to the UK data protection requirements.

To ensure the network is used safely, this school:

- Makes clear that no one should log on as another user
- Requires all users to always log off when they have finished working
- Makes clear that staff are responsible for ensuring that any computer, tablet or laptop loaned to them by the school, is used solely to support their professional responsibilities.
- Maintains equipment to ensure Health and Safety is followed;
- Ensures that access to the school's network resources from remote locations by staff is restricted and access is only through school approved systems:
- Does not allow any outside agencies to access our network remotely except where there is a clear professional need and then access is restricted and is only through approved systems; e.g. technical support
- Has a clear disaster recovery system in place for critical data that includes a secure, remote back up of critical data;
- Our wireless network has been secured to appropriate standards suitable for educational use;
- All computer equipment is installed to a professional standard and meets health and safety standards;
- Reviews the school ICT systems regularly with regard to health and safety and security

Passwords policy

- All admin staff have their own unique username and private passwords to access school systems. Staff are responsible for keeping their password private and to change it when required.

Personal mobile phones and mobile devices

- Student mobile phones and personally-owned devices should only be used for learning purposes if requested by the teacher in class time. They should be in during class time.
- Mobile phones and personally-owned mobile devices brought in to school are the responsibility of the device owner. The school accepts no responsibility for the loss, theft or damage of personally-owned mobile phones or mobile devices.

Personal Use of Systems

The school permits the incidental personal use of school IT and other equipment provided that**:**

- use must be minimal and take place out of normal working hours (that is, during a usual lunch hour, before or after standard work hours);
- it does not interfere in any way with the User carrying out their duties on behalf of the school;
- it does not commit the school to any marginal costs; and
- it complies with the school's policies including this policy.

- The policy to allow continued personal use is dependent upon its not being abused and the school reserves the right to withdraw permission from any User, group of Users or all Users or to amend the scope of this policy at any time and at its absolute discretion.
- Misuse or abuse of school equipment in breach of this policy will be dealt with in accordance with our disciplinary procedure. Serious breaches may amount to gross misconduct which can lead to summary dismissal. Misuse can, in certain circumstances, constitute a criminal offence and may result in a report to the police.

School website

- Any photographs published on the web from January 2019 are published with the written approval of the people in them and do not have full names attached;
- We do not use students' names when saving images in the file names or in the tags when publishing to the school website.

Social media and social networking

Staff are required to not post entries that are publicly accessible, which contain negative references to the company, its staff, business activities, clients or products.

Staff must not conduct themselves in a way that is detrimental to the company. Staff must take care not to allow their interaction on social networking websites to damage working relationships between members of staff and the company's clients or third parties.

Staff must not 'add' any students to their personal social networks. Concern regarding students' use of social networking, social media, and personal publishing sites (in or out of CELT) will be raised with their parents / group leaders, particularly when concerning students underage use of sites.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff will be issued with a school phone where contact with students, parents or carers is required.
- Mobile Phones and personally-owned devices should be switched to 'silent' mode during class time.
- Where staff members are required to use a mobile phone for school duties, for instance in case of emergency during off-site activities, or for contacting students or parents, then a school mobile phone will be provided and used. In an emergency where a staff member doesn't have access to a school-owned device, they should use their own device and hide (by inputting 141) their own mobile number for confidentiality purposes.

8. Other relevant policies:

- Safeguarding Policy and Code of Conduct
- GDPR Policy