

Equine Learning CIC (ELCIC) – E-safety Policy

1. Aims

ELCIC aims to:

- Have robust processes in place to ensure the online safety of students, staff and volunteers.
- Deliver an effective approach to online safety, which empowers us to protect and educate the learning provision in its use of technology
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

2. Legislation and guidance

This policy is based on the Department for Education's statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on preventing and tackling bullying and searching, screening and confiscation. It also refers to the Department's guidance on protecting children from radicalisation. It reflects existing legislation, including but not limited to the Education Act 1996 (as amended), the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so. The policy also takes into account the National Curriculum computing programmes of study.

3. Roles and responsibilities

The Director

The Director has overall responsibility for monitoring this policy and holding the ELCIC team to account for its implementation. The Director will:

- Ensure that they have read and understand this policy
- Agree and adhere to the terms on acceptable use of the ICT devices and the internet (appendix 2)
- Be responsible for ensuring that staff understand this policy, and that it is being implemented consistently.
- As DSL takes lead responsibility for online safety in school, in particular:
 - ensuring that staff understand this policy and that it is being implemented consistently
 - Working with staff, as necessary, to address any online safety issues or incidents
 - Ensuring that any online safety incidents are logged (see appendix 4) 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 ELCIC behaviour policy
 - Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the ELCIC behaviour policy
- Liaising with other agencies and/or external services if necessary

This list is not intended to be exhaustive.

The Education Programme Supervisor is responsible for:

- Putting in place appropriate filtering and monitoring systems, which are updated on a regular basis and keep students safe from potentially harmful and inappropriate content and contact online while at ELCIC, including terrorist and extremist material
- Ensuring that Students at Equine Learning CIC only have access to the internet during supervised sessions and are never left alone with ICT equipment
- Ensuring that ELCIC's ICT equipment is secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy

This list is not intended to be exhaustive.

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 ELCIC's ICT equipment / system and the internet (appendix 2), and ensuring that students follow ELCIC's terms on acceptable use (appendix 1)
- Working with the DSL to ensure that any online safety incidents are logged (see appendix 4) and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the ELCIC behaviour policy
-

This list is not intended to be exhaustive.

Parents are expected to:

- Notify a member of staff or the Director of any concerns or queries regarding this policy
- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT system /equipment and internet (appendix 1)

Parents can seek further guidance on keeping children safe online from the following organisations and websites:

- What are the issues? UK Safer Internet Centre: <https://www.saferinternet.org.uk/advice-centre/parents-and-carers/what-are-issues>
- Hot topics, Childnet International: <http://www.childnet.com/parents-and-carers/hot-topics>
- Parent factsheet, Childnet International: <http://www.childnet.com/ufiles/parents-factsheet-09-17.pdf>

Visitors and members of the community

Visitors and members of the community who use the school'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 (appendix 2).

4. Educating students about online safety

Students will be taught about online safety as part of their learning sessions. Students will gain an understanding of:

- a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy

- recognising inappropriate content, contact and conduct, and know how to report concerns
- how changes in technology affect safety, including new ways to protect their online privacy and identity
- How to report a range of concerns
- The safe use of social media and the internet will also be covered where relevant.

ELCIC will use learning time to raise students' awareness of the dangers that can be encountered online and may also invite speakers to talk to students about this. ELCIC should ensure that the use of Internet derived materials by staff and by students complies with copyright law. Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy. Students will be taught to acknowledge the source of information used and to respect copyright when using Internet material in their own work.

Managing Internet Access: Information system security

- The security of the school information systems will be reviewed regularly.
- Virus protection will be installed and updated regularly.
- Files held on ELCIC's devices will be regularly checked.

E-mail

- Students will not be expected to use email at ELCIC.
- Students will be encouraged to understand that they must not reveal personal details of themselves or others in e-mail communication or arrange to meet anyone without specific permission.
- E-mail sent to external organisations as part of any learning should be written carefully and authorised before sending, in the same way as a letter written on school headed paper. The forwarding of chain letters is not permitted.

Published content and the school web site

- The contact details for ELCIC on the website is the address, e-mail and telephone number. Staff or student's personal information will not be published.
- The Director has website editorial control will ensure that content is accurate and appropriate. The Website should comply with guidelines for publications including respect for intellectual property rights and copyright.

Publishing staff and student's images and work

- Photographs that include students will be selected carefully and will not enable individual students to be clearly identified by name.
- Students' full names will not be used anywhere on the Web site, particularly in association with photographs.
- Written permission from parents or carers will be obtained before photographs of students are published on the school Web site.
- Student's work can only be published with the permission of the student and parents. Images of staff should not be published without consent.

Social networking and personal publishing

- Social networking sites and newsgroups will be blocked unless a specific use is approved.
- Students are advised never to give out personal details of any kind which may identify them or their location. Examples would include real name, address, mobile or landline phone numbers, school, IM address, e-mail address, names of friends, specific interests and clubs etc.

- Teachers' official blogs / social media accounts will be password protected and run from the school portal.
- Teachers should be advised not to run social network spaces for students on a personal basis.
- Students should be advised not to place personal photos on any social media space. They should consider how public the information is and consider using private areas. Advice should be given regarding background detail in a photograph which could identify the student or his/her location e.g. house number, street name, school.

5. Cyber-bullying

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. (See also the ELCIC behaviour policy) Students are not permitted to access the internet on their phone or have unsupervised access to the internet during learning time or at any other time during their time at ELCIC.

Preventing and addressing cyber-bullying

To help prevent cyber-bullying, we will ensure that students understand what it is and what to do if they become aware of it happening to them or others. We will ensure that students know how they can report any incidents and are encouraged to do so, including where they are a witness rather than the victim. The school will actively discuss cyber-bullying with students, explaining the reasons why it occurs, the forms it may take and what the consequences can be. Teachers will discuss cyber-bullying with students during learning time.

All staff and volunteers (where appropriate) receive awareness training on cyber-bullying, its impact and ways to support students, as part of safeguarding training. In relation to a specific incident of cyber-bullying, ELCIC will follow the processes set out in the school behaviour policy. Where illegal, inappropriate or harmful material has been spread among students, ELCIC 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.

Examining electronic devices

School staff have the specific power under the Education and Inspections Act 2006 (which has been increased by the Education Act 2011) to search for and, if necessary, delete inappropriate images or files on students' electronic devices, including mobile phones, iPads and other tablet devices, where they believe there is a 'good reason' to do so.

When deciding whether there is a good reason to examine or erase data or files on an electronic device, staff must reasonably suspect that the data or file in question has been, or could be, used to:

- Cause harm, and/or
- Disrupt learning, and/or
- Break any of the ELCIC policies

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 school discipline),
- and/or report it to the police

Any searching of students will be carried out in line with the DfE's latest guidance on screening, searching and confiscation. Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the ELCIC complaints procedure.

6. Acceptable use of the internet at ELCIC

- Students will only have supervised access to the internet during learning time.
- All students, parents, staff, volunteers and governors are expected to sign an agreement regarding the acceptable use of ELCIC's ICT system and the internet (appendices 1 and 2).
- Visitors will be expected to read and agree to ELCIC's terms on acceptable use if relevant.
- Use of ELCIC internet must be for educational purposes only, or for the purpose of fulfilling the duties of an individual's role.
- We will monitor the websites visited by students, staff, volunteers, and visitors (where relevant) to ensure they comply with the above.

More information is set out in the acceptable use agreements in appendices 1 and 2.

7. Students using mobile devices in school

Students may bring mobile devices into ELCIC but are not permitted to use them at all whilst on the premises unless with the permission of a member of staff. The mobile phones must be handed to The Education Programme Supervisor who will put the mobile device in a locker and hand it back at the end of the day. Full details can be found in the mobile phone policy. Any use of mobile devices at ELCIC by students must be in line with the acceptable use agreement (see appendix 1). Any breach of the acceptable use agreement by a student may trigger disciplinary action in line with the ELCIC behaviour policy, which may result in the confiscation of their device.

8. Staff using work devices outside ELCIC

Staff members using a work device outside ELCIC must not install any unauthorised software on the device and must not use the device in any way which would violate ELCIC's terms of acceptable use, as set out in appendix 2. Staff must ensure that their work device is secure and password-protected, and that they do not share their password with others. They must take all reasonable steps to ensure the security of their work device when using it outside ELCIC. If staff have any concerns over the security of their device, they must seek advice from the Director. Work devices must be used solely for work activities.

How the school will respond to issues of misuse

- Where a student misuses ELCIC's ICT systems, device or internet, we will follow the procedures set out in the behaviour policy. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident, and will be proportionate.
- Where a staff member misuses ELCIC'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 disciplinary procedures. The action taken will depend on the individual circumstances, nature and seriousness of the specific incident.
- ELCIC will consider whether incidents which involve illegal activity or content, or otherwise serious incidents, should be reported to the police.

9. Training

All new staff members will receive training, as part of their induction, on safe internet use and online safeguarding issues. All staff members will receive refresher training at least once each academic year as part of safeguarding training. The DSL and safeguarding team will undertake child protection and safeguarding training, which will include online safety, at least every 2 years. Volunteers will receive appropriate training and updates, if applicable. More information about safeguarding training is set out in our safeguarding policy.

12. Monitoring arrangements

- The DSL logs behaviour and safeguarding issues related to online safety.
- This policy will be reviewed every 2 years.

13. Links with other policies

This online safety policy is linked to our:

- Safeguarding policy
- Behaviour policy
- Staff disciplinary procedures
- Data protection policy and privacy notices
- Complaints procedure
- Anti-bullying policy



Appendix 1: Acceptable use agreement (students and parents/carers)

Student ICT Acceptable Use Policy

- I will only use ICT systems at ELCIC, including the internet, e-mail, digital video, mobile technologies, etc. for school purposes.
- I will not download or install software on school technologies.
- I will only log on to the ELCIC Learning Platform with my own user name and password.
- I will follow security systems and not reveal my passwords to anyone
- I will make sure that all ICT communications with students, teachers or others is responsible and sensible.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my coach.
- I will not give out any personal information of any kind which may identify me or give my location; such as my real name, phone number, home address, email address or names of friends or similar details relating to another student or member of staff.
- Images of students and/ or staff will only be taken, stored and used for school purposes in line with school policy and not be distributed outside the school network without the permission of the coach in charge. Images will be deleted after 2 years.
- I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring any of the aforementioned into disrepute.
- I will respect the privacy and ownership of others' work on-line at all times.
- I will not attempt to bypass the internet filtering system.
- I understand that all my use of the Internet and other related technologies will be supervised by a coach or support worker.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied, and my parent/ carer may be contacted.

Dear Parent/ Carer

ICT including the internet and learning platforms are part of learning at ELCIC. We expect all students to be safe and responsible when using ICT. It is essential that students are aware of e-safety and know how to stay safe when using any ICT. Students are expected to read and discuss the Student ICT Acceptable Use Policy with their parent or carer and then to sign and follow the terms of the policy. Any concerns or explanation can be discussed with the Education Programme Supervisor. Please return a signed copy of this form to ELCIC

Student and Parent/ carer signature

We have discussed the Student ICT Acceptable Use Policy document and

.....(student name)
agrees to follow the eSafety rules and to support. the safe and responsible use of ICT at ELCIC.

Parent/ Carer Signature

Student Signature.....Date



Appendix 2: Acceptable use agreement (staff, volunteers and visitors)

Staff and Visitor Acceptable Use Agreement / Code of Conduct

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life at ELCIC. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere, at all times, to its content. Any concerns or clarification should be discussed with the Education Programme Supervisor or the Director.

- I will only use ELCIC’s email / Internet / Slack / Learning Platform / booking system and any related technologies for professional purposes or for uses deemed ‘reasonable’ by the Director
- I will comply with the ICT system security and not disclose any passwords provided to me by the Director or other related authorities
- I will ensure that all electronic communications with students and staff are compatible with my professional role.
- I will not give out my own personal details, such as mobile phone number and personal e-mail address, to students.
- I will only use the approved Learning Platform, Slack, booking system and the secure e-mail system(s) for any ELCIC business.
- I will ensure that personal data (such as data held on MIS software) is kept secure and is used appropriately, whether in the building, taken off site or accessed remotely. Personal data can only be taken out of the building or accessed remotely when authorised by the Director. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software without permission of the Director.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of students and/ or staff will only be taken, stored and used for professional purposes in line with ELCIC policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the ELCIC network without the permission of the parent/ carer, member of staff or Director.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or the Director. I give consent for private chat channels in Slack to be monitored and checked if required
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in ELCIC and outside ELCIC, will not bring my professional role or the organisation into disrepute.
- I will support and promote ELCIC’s e-Safety and Data Security policies and help students to be safe and responsible in their use of ICT and related technologies.
- Any personal costs incurred through the use of ELCIC technology i.e. ELCIC issued mobile phones, will be charged directly to the staff member and action taken for inappropriate use

User Signature

I agree to follow this code of conduct and to support the safe and secure use of ICT at ELCIC

Signature Name.....Date

Job title



EQUINE LEARNING
COMMUNITY INTEREST COMPANY

Appendix 3:
Online Safety Incident Report Log

Date of incident	
Name of staff member completing this log	
Where the incident took place	
Description of the incident	
Any action taken	
Name of the manager this form was handed to	
Manager action	
Further action needed	