APPROVED CENTRE

Rainbow Horses

Learning Centre CIC

Online Safety Policy 2023

Introduction

Learners who attend Rainbow Horses Learning Centre are increasingly accessing the internet in a variety of ways including, via Smartphones, tablets or laptop computers.
Learners will either have their own equipment which can access the internet or will use the centre's equipment. A centre's equipment is often for personal as well as business use.

Significant educational benefits can result from internet use, including access to information from around the world and the ability to communicate widely (eg with EAQ centres in Australia). Internet safety depends on staff, parents/carers to taking responsibility for the use of the Internet.

Purpose

The purpose of internet use in equine assisted learning sessions is to raise educational standards, to promote learner achievement and to support the professional work of staff. Benefits of using the internet allows access to world-wide educational resources including the EAQ Network Channel for online videos for horse awareness and it is important that staff take reasonable precautions to ensure that learners access only appropriate material.

- Learners will be supervised at all times whilst on the internet
- Rules for internet access will be made clear to learners

Roles and Responsibilities

The following section outlines the roles and responsibilities for online safety of individuals and groups within the Rainbow Horses:

Directors:

- Directors are responsible for the approval of the Online Safety Policy and for reviewing the effectiveness of the policy.

- ensures that the School has appropriate filters and monitoring systems in place and regularly reviews their effectiveness by reviewing reports from the safeguarding team.

CEO and Senior Leaders:

- The DSL and DDSL are responsible for ensuring the safety (including Online Safety) of members of Rainbow Horses community
- The CEO and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious Online Safety allegation being made against a member of staff.

Online safety is recognised as an essential aspect of strategic leadership in Rainbow Horses and the CEO, with the support of Directors, aims to embed safe practices into the culture. The CEO, DSL and DDSL ensures that the policy is implemented and compliance with the policy monitored. The responsibility for Online Safety has been designated to a member of the senior management team.

Designated Safeguarding Lead

The Designated Safeguarding Lead (Sue Coombes) is trained in Online Safety issues and is aware of the potential for serious child Protection issues to arise from:

- sharing of personal data
- access to illegal/inappropriate materials
- inappropriate on-line contact with adults/strangers
- potential or actual incidents of grooming
- cyber-bullying

Teaching and Support Staff

All staff are responsible for promoting and supporting safe behaviours and following online safety procedures. Central to this is fostering a 'no blame' culture so pupils feel able to report any bullying, abuse or inappropriate materials.

All staff are also responsible for ensuring that:

- they have an up to date awareness of Online Safety matters and of the current online Safety policy and practices
- they report any suspected misuse or problem to the Online Safety Co-ordinator or senior leader for investigation, action and possible sanction

All staff should be familiar with the policy including:

- Safe use of e-mail
- Safe use of Internet including use of internet-based communication services, such as instant messaging and social network
- Safe use of network, equipment and data
- Safe use of digital images and digital technologies, such as mobile phones and digital cameras
- publication of learner information/photographs and use of website
- Online bullying procedures
- Their role in providing Online Safety/acceptable ICT use education for learners
- Their role in preventing terrorism and extremism

Staff are reminded / updated about Online Safety matters at least once a year.

Learners

- are responsible for using the ICT systems and mobile technologies in accordance with the learner Acceptable Use Policy, which they will be expected to sign before being given access to systems
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

We include Online Safety in the curriculum and ensure that every learner has been educated about safe and responsible use. Learners need to know how to minimise online risks and how to report a problem.

Parents/Carers

Rainbow Horses will help to support parents and carers to understand these issues through parents' evenings, newsletters, letters, website and information about national/local Online Safety campaigns and literature. Parents and carers will be responsible for:

- Notify a member of staff or the DSL of any concerns or queries regarding this policy;

Visitors and Members of the Community

Visitors and members of the community who use the 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 of the Appropriate Use Policy

Education – Learners

Online Safety education will be provided in the following ways

- A planned Online Safety programme is provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside
- Key Online Safety messages will be reinforced as part of a planned programme
- Learners will be taught to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

Education & Training – Staff

It is essential that all staff receive Online Safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- All staff will receive Online Safety training as part of their training programme, ensuring that they fully understand the Online Safety policy and Acceptable Use Policies.

Acceptable Use

Use of centre computers or equipment that can access the internet by learners must be in support of the aims and objectives of the curriculum.
When using the internet, all users are expected to comply with all laws and government regulations concerning copyright, libel, fraud, discrimination and obscenity and all centre staff are expected to communicate in a professional manner consistent with the rules of behavior contained in the Code of Conduct.

Whilst using the internet learners should be supervised. However, when appropriate to their age and their focus of study, learners may pursue electronic research independent of staff (written permission is required from their parent / guardian). In all cases pupils should be reminded of their responsibility to use these resources in line with the centre's policy on acceptable Use.

Facilitators should use the internet to enhance and develop learner interests, model appropriate and effective use, and provide guidance and instruction to learners in the acceptable use of the internet.

Sexting/Peer on Peer Abuse/Cyberbullying

All staff should be aware that safeguarding issues can manifest themselves via peer on peer abuse. This could include cyberbullying and sexting (youth produced sexual imagery). Staff should be clear as to the policy and procedures with regards to peer on peer abuse and sexual harassment.

Further guidance on Sexting and Cyberbullying and how to handle incidents can be found below:

https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/551575/6.2439_KG_NCA_Sexting_in_Schools_WEB__1_.PDF

https://www.gov.uk/government/publications/preventing-and-tackling-bullying

Examining Electronic Devices –

If an incident comes to your attention report it to the DSL immediately.

Never view, copy, print, share, store or save the imagery yourself, or ask a child to share or download – **this is illegal**.

Please refer to the DSL, the safeguarding procedures and the UKCIS guidance for further information and advice.
Any complaints about searching for or deleting inappropriate images or files on pupils' electronic devices will be dealt with through the complaints procedure.
Adults should not view youth produced sexual imagery unless there is good and clear reason to do so.

If the capture involves Child Abuse images (or suspected child abuse images):

- Do not search or check a device for further images. The device should be confiscated and further advice should be sought from the DSL.
- Do not print or copy images.
- Do not email a copy of the image to anybody.
- Do not show the image/capture to a minor.
- Do not show the image on the system to anybody who does not need to be exposed to the image.

Any printing, emailing or copying of a child abuse image is an offence under English Law. A child abuse image or indecent image of a child is an image of a sexual nature which depicts a child under the age of 18. If the capture involves Adult pornography:

- Do not search or check a device for further images. The device should be confiscated and further advice should be sought from the DSL.
- Do not print out or copy images out unless necessary

- Do not email a copy of the image to anybody, unless necessary
- Do not show the image on the system to anybody who does not need to be exposed to the image.
- Do not show the image/capture to a minor.

An offence against English law may be committed if adult pornography image is shown to a child. If there is a need to print out the image to show an adult this must be kept secure and not for general circulation.

Technical infrastructure- Filtering and Monitoring

Rainbow Horses will do all that they reasonably can to limit learners exposure to the risks below in regards to online material:

-content: being exposed to illegal, inappropriate or harmful material;

-contact: being subjected to harmful online interaction with other users; and

-conduct: personal online behaviour that increases the likelihood of, or causes, harm.

As part of this process Rainbow Horses has appropriate filters and monitoring systems in place. The appropriateness of these filters will be considered and governors and proprietors will consider a whole community approach to online safety.

Awareness
It is possible for the centre to set up controls so that learners are able to access only certain websites. However, once a site has been accessed eg YouTube, for acceptable purposes, it is easy to access other, less suitable material.
If you come across any offensive web pages please report this to CEOP (www.ceop.police.uk)

Directors and senior staff will ensure that all staff undergo regularly updated safeguarding training and that online safety training for staff is integrated, aligned and considered as part of the overarching safeguarding approach.

- technical systems will be managed in ways that ensure that Rainbow Horses meets recommended technical requirements.
- There will be regular reviews and audits of the safety and security of technical systems.
- Servers, wireless systems and cabling must be securely located and physical access restricted.
- All users will have clearly defined access rights to technical systems and devices.
- The “master / administrator” passwords for the ICT system, must also be available to the CEO or other nominated senior leader and kept in a secure place (e.g. safe).
  The IT Manager (or nominated SLT member) is responsible for ensuring that software licence logs are accurate and up to date and that regular checks are made to reconcile the number of licences purchased against the number of software installations.
- Internet access is filtered for all users. Illegal content (child sexual abuse images) is filtered by the broadband or filtering provider by actively employing the Internet Watch Foundation’s Child Abuse Image Content (CAIC) list. Content lists are regularly updated and internet use is logged and regularly monitored. There is a clear process in place to deal with requests for filtering changes.
- Rainbow horses has provided enhanced / differentiated user-level filtering.

- Rainbow Horses staff regularly monitor and record the activity of users on the technical systems
- Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, work stations, mobile devices etc. from accidental or malicious attempts which might threaten the security of the systems and data. These are tested regularly. The infrastructure and individual workstations are protected by up to date virus software.
- An agreed procedure is in place for the provision of temporary access of "guests" (e.g.visitors) onto the systems.
- An agreed policy is in place regarding the extent of personal use that users (staff / pupils / community users) and their family members are allowed on Rainbow Horses devices that may be used out of the centre.

Online activities which are encouraged include:
• The use of email and computer conferencing for communication between learners and staff.
• Use of the internet to investigate and research subjects, themes or topics
• Use of the internet to investigate careers
• The development of pupils' competence in ICT skills and their general research skills.

Online activities which are not permitted include:
• Searching, viewing or retrieving materials that are not related to the aims of the curriculum or future careers.
• Copying, saving or redistributing copyright-protected material, without approval.
• Subscribing to any services or ordering any goods or services, unless specifically approved by the centre.
• Playing computer games or using other interactive 'chat' sites unless specifically approved by the centre.

Those with access to the internet must not:
• Retrieve, send, copy or display offensive messages or pictures
• Use obscene or racist language
• Harass, insult or attack others
• Damage computers, computer systems or computer networks
• Violate copyright laws
• Use another user's password
• Trespass in another user's folders, work or files
• Publish, share or distribute any personal information about other learners or staff (such as: home address; email address; phone number; etc) without their express consent
• Download software unless requested to do so
• Reveal personal details such as age, address of themselves or other learners.

Guidelines
Learners will:
• Have access to email in a safe and secure environment.
• Have access to a variety of approved websites.
• Be taught the skills in order to use internet and email as an ICT tool.
• Use internet and email to support, enhance and develop all aspects of curriculum.
• Develop internet and email skills at the appropriate level regardless of race, gender, intellect and emotional or physical difficulties.

*

Guidance on the use of Social Media

Many learners access social media sites such as Facebook and YouTube. Centres often have a Facebook page on which they provide details of what has been happening during sessions.
Learners may only have images of themselves placed on these centre pages if they have agreed to this in writing and given their informed consent. Parents must agree in the case of learners who are under 18.
Learners may not place images of other learners onto any site whatsoever, unless they can show that they have permission to do so from the learner concerned.

Use of email

Care should be taken when emailing individual learners and it is advised that centres copy parents / carers in on these messages in order to protect themselves and the individual learner concerned.

Data Protection

Rainbow Horses has a Data Protection Policy and Compliance Procedures for Staff and an which all staff should be familiar with, to make sure that personal data is kept safe when working in or off-site and using personal devices. Please refer to those policies for further detail. Regular staff and learner training on information security is provided.

Responding to online safety incidents

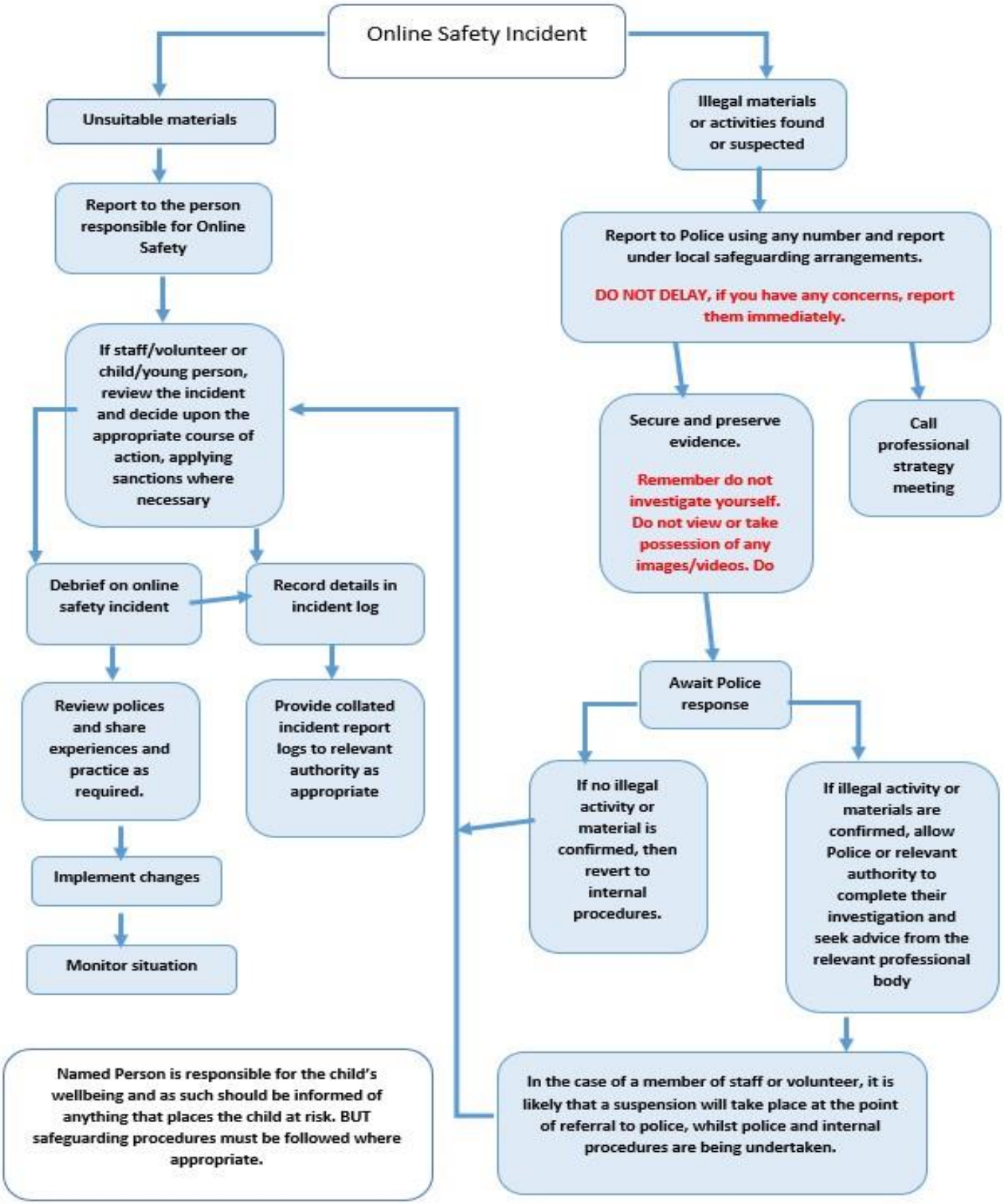
The following guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities; please see Appendix 1 for clarification of acceptable / unacceptable / illegal online activities.

Resources

There are excellent resources and training available for centres and these are highly recommended for all staff who have learners who are likely to access the internet.
http://ceop.police.uk/Knowledge-Sharing/
https://www.thinkuknow.co.uk/teachers/
http://www.nspcc.org.uk/
www.thinkuknow.co.uk
www.disrespectnobody.co.uk
www.saferinternet.org.uk
www.internetmatters.org
www.childnet.com/cyberbullying-guidance
www.pshe-association.org.uk
http://educateagainsthate.com
www.gov.uk/government/publications/the-use-of-social-media-for-onlineradicalisation

Signed: Sue Coombes, CEO
Reviewed on: August 2023
Next review due: August 2024

APPENDIX 1-


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.