The HOLT Isle of Wight Online Safety Policy

Overview

This policy is to safeguard and protect all members of The HOLT’s online community by providing a framework to promote and maintain a safe, effective and responsive online safety culture. It applies to all members of The HOLT, including the Director, employees, clients, volunteers, visitors and community users who have access to the HOLT, and are users of The HOLT’s digital technology systems, both internally and externally.

Contents

* Introduction
* Online Safety statement
* Scope
* Roles and Responsibilities
* Education and training
* Cultivating a safe environment
* Responding to online safety concerns
* Responding to complaints
* Monitoring and compliance
* Approval process
* Dissemination and communication process
* Development of the policy

Introduction

Online safety in training centres is of paramount importance. As the online world evolves, so do both the online harms and risks facing our clients, and the relevant legislation, both statutory and non-statutory, which directs and guides how training centres and colleges should meet their online safety requirements.

Employees and Trustees play a vital role in setting an example for The HOLT, and are central to implementing policy and process. It is imperative that we approach online safety as a whole community and that all stakeholders are aware of their responsibilities and duties in relation to keeping our vulnerable clients safe online. This will support a robust online safety ethos and ensure that we are providing the best online safety provision that we possibly can.

Online Safety Statement

The HOLT asserts that online safety is an essential element of safeguarding our clients and duly acknowledges its statutory obligation to ensure that all our clients and staff are protected from potential online harm.

The HOLT believes that the internet and associated devices are an integral part of everyday life and clients must be supported and empowered to build resilience and to develop strategies to recognise and respond to online risks.

Policy scope

Online safety is an omnipresent topic which requires recurrent regulatory review and places a stringent duty of care on us all. This policy supports training centres and colleges in meeting statutory requirements as per DFE guidance under KCSIE, Working together to safeguard Children and non statutory guidance, and teaching online Safety in Schools. Effective, timely and robust online safety is fundamental to protecting young people in education and it is a significant part of the safeguarding agenda.

High quality online safety provision requires constant vigilance and a readiness to act where abuse, exploitation or neglect is suspected. The landscape of safeguarding is constantly evolving, and educational establishments must endeavour to embrace and shape their key priorities in support of this. Education has a vital role to fulfil in protecting young people and adults from forms of online abuse whilst demonstrating a concerted obligation to respond with haste and flexibility to concerns as they arise. Above all, employees must foster dedication to ensuring that they listen to the voices of the vulnerable and act upon what is heard. Safeguarding is everyone’s responsibility.

Hidden Harms – types of online abuse may include

Cyberbullying

Emotional abuse

Grooming

Sexting

Sexual abuse

Sexual exploitation

The types, patterns and different circumstances of significant harm and abuse should be considered within the categories identified for young people in the Children Act 2004. These are

Neglect

Sexual

Physical

Emotional

Technology can facilitate a world of learning and development in addition to helping yield a range of opportunities. However the stark reality is that it can also present a window to potential and actual harm and abuse. It can elicit and support an array of illegal abusive behaviours including, but not limited to:

Harassment

Stalking

Threatening behaviour

Creating or sharing child sexual abuse material

Inciting a child to sexual activity

Sexual exploitation

Grooming

Sexual communication with a child

Causing a child to view images of watch videos of a sexual act

This policy should be read alongside the relevant policies relating to safeguarding of clients and in addition the associated statutory legislation and guidance as stipulated on page 1-2 of this policy.

Roles and Responsibilities

All Employees, Trustees and the Director are responsible for protecting our clients online. This includes every member of staff who works at the school, including office staff and cleaning staff. All working at HOLT should always act in accordance with their own professional boundaries, upholding professional behaviour and conduct at all times.

All employees and the Director should:

Be aware of and adhere to all policies which support online safety and safeguarding.

Contribute to policy development and review

Support in the ownership and responsibility for the security of systems and the data accessed

Model good practice when using technology

Know the process for making referrals and reporting concerns

Know how to recognise, respond and report signs of online abuse and harm

Receive appropriate child and adult protection training

Always act in the best interest of the clients

Be responsible for their own continuing professional development in online safety.

Trustees

The Trustees’ role for online safety at the HOLT includes but is not limited to:

Upholding online safety as a safeguarding issue which is embedded across the whole HOLT culture

Ensuring that Clients are provided with a safe environment in which to learn and develop

Ensuring that the HOLT has appropriate filters and monitoring systems in place

Ensuring that the HOLT has effective policies and training in place

Carrying out risk assessments on effectiveness of filtering systems

Auditing and evaluating online safety practice

Designated Safeguarding Lead and Deputy Designated Safeguarding Lead

With respect to online safety it is the responsibility of the DSL to:

Ensure that clients are being appropriately taught about and know how to use the internet safely and responsibly

Ensure that employees are aware of measures to keep clients safe online through relevant training provision

Take responsibility for all safeguarding matters, including online safety

Collaborate with the Trustees

Facilitate effective record keeping and the reporting and monitoring of all online safety concerns

Promote online safety and the adoption of a combined approach

Maintain own training and learning needs, ensuring they are up to date with all matters relating to online safety

Clients

With respect to online safety at The HOLT, clients, where able, need to:

Know who the DSL is

Engage in age appropriate online safety education opportunities

Contribute to policy development and review

Read and adhere to online safety policies and acceptable use policies where able

Respect the feelings of others, both off and online

Take responsibility for keeping themselves and others safe online

Know where and how to find help with any online incidents or concerns

Know how, when and where to report concerns and when to seek help from a trusted employee of the HOLT or other adult

The UKCCIS Education for a connected world framework aims to equip young people for digital life and covers

Self image and identity

Online relationships

Online reputation

Online bullying

Managing online information

Health, wellbeing and lifestyle

Privacy and security

Copyright and ownership

Parents and Carers

Parents and carers need to understand the risks that their young people face online to protect them from online dangers. They need to:

Read and adhere to all relevant policies

Be responsible when taking photos/using tech at events provided by the HOLT

Know who the DSL is for The HOLT

Know how to report online issues

Support online safety approaches and education provision

Be a role model for safe and appropriate behaviour

Identify changes in behaviour that could indicate that their child is at risk of online harm or abuse

Education and Training

Safeguarding activity across the UK continues to intensify in volume and intricacy with national influences relating to political uncertainty, a rise in poverty, an increase in the ageing population, sustained funding pressures and increased demand for child and adult services.

Furthermore, a commitment to ensuring the provision of an integrated and highly robust safeguarding service for all ages is essential. Effective online safety provision and promotion of the welfare of clients relies upon constructive relationships that are conducive to robust multi-agency partnership working. This can only be effective when all staff are knowledgeable, confident and equipped with the skills to deal with processes and procedures when concerns arise relating to online abuse and harm.

Online safety has a high emphasis on a competent well established workforce, up to date policies and procedures, robust governance arrangements and collaborative practices. Types of online risk usually fall into one of three categories.

Contact: Contact from someone online who may wish to bully or abuse the client. This could also include online grooming, online harassment, or activities of a commercial nature, including tracking and harvesting personal information.

Content: Inappropriate material available to children online including: adverts, spam, sponsorship, personal info, violent or hate content, pornographic or unwelcome sexual content, biased materials, racist materials and misleading information and advice.

Conduct: The client may be the perpetrator of activities, including illegal downloading, hacking, gambling, financial scams, bullying or harassing another client. They might create and upload inappropriate materials or provide misleading information or advice.

Education

The HOLT will provide opportunities for clients to engage with learning around:

Safe and responsible use and access of the internet

Online Safety

Evaluation of content

Online behaviour for safety

Online risks

Pornography and it’s harms

Awareness of Techniques used to persuade

How and when to seek support

These will be delivered at an appropriate level for the clients’ understanding.

Responding to online safety concerns

The safety of clients is of paramount importance. Immediate action may be required to safeguard investigations and any other clients. Any concern that clients may be at risk of harm or abuse must be immediately reported. Reputational issues must be managed appropriately by discussion with the relevant communications team.

Online safety is recognised as part of the HOLTs safeguarding responsibilities. The DSL will take lead responsibility for online safety concerns which should be recorded and actioned. Clients will be enabled to share online concerns.

If there is immediate danger, phone 999

Inform and refer to all appropriate agencies

Always adhere to the HOLT’s safeguarding procedures and report to the DSL asap.

Responding to complaints

There are a number of sources from which a complaint or allegation might arise, including those from

* A client
* An adult
* A parent/carer
* A member of the public
* An employee

There may be up to three components in the consideration of an allegation.

A police investigation of a possible criminal offence

Enquiries and assessment by children’s social care or adult social care relating to whether a child or an adult at risk is in need of protection or services

Consideration by the HOLT of disciplinary action in respect of the individual, including suspension.

It is the responsibility of the member of staff to inform the Director if they are being investigated in relation to children or adults at risk with respect to protection concerns outside of work. They should also report if their own children, or children they live with become subject to child protection matters, or an adult related to them or living with them become subject to adult protection matters.

Monitoring and Compliance

Monitoring will be carried out in a variety of forms, including analysing incident logs, checking planning for online safety training and stakeholder questionnaires. Monitoring will be conducted by the DSL and the safeguarding Trustee annually.

Sources

Children Act 1989

Children Act 2004

Computer Misuse Act 1990

Criminal Justice and Courts Act 2015

Data Protection Act 1998

Education Act 2011

Education and Inspections Act 2006

Freedom of Information Act 2000

Malicious Communications Act 1988

Serious Crime Act 2015

Voyeurism (offences) Act 2019