



Employment, Learning and Skills Division

ONLINE SAFETY POLICY

Adult Learning Service



Ver3:Dec22

Name of Policy	Online Safety Policy
Author	Kelly Arrowsmith Quality and Learner Experience Manager
For approval by	E.L.S. Divisional Management Group
Date of approval	9 TH December 2022
Frequency of review	Biennial (or sooner in response to incident/cause for concern)
Next review date	August 2024
Total No. of pages (Inc. appendices)	10
Comments	Version 3 Linked Policies: Adult Learning Learner Disciplinary Policy and Procedure (2022) HBC Acceptable Use Policy (2018) Adult Learning Acceptable Use Policy (2022) Corporate Information Governance Handbook (2019) HBC Safeguarding Adults Procedures (2022) Adult Learning Safeguarding Adults (including Prevent) Policy (2022)

Contents

ONLINE SAFETY POLICY	4
SCOPE OF THE POLICY	4
MONITORING AND REVIEW	4
ROLES AND RESPONSIBILITIES	5
<i>Management Team</i>	5
<i>The Safeguarding Lead</i>	5
<i>Governors</i>	6
<i>Halton Borough Council ICT Team</i>	6
<i>Adult Learning Staff</i>	6
TECHNICAL SUPPORT	7
LEARNERS	7
USEFUL INFORMATION	8
<i>Safeguarding</i>	8
<i>Data Protection</i>	9
<i>Communications</i>	9
<i>Social Media</i>	10
APPENDIX 1 - ONLINE SAFETY INCIDENT FLOWCHART	11
APPENDIX 2 - QUESTIONS TO SUPPORT ASSESSMENT (UNDER 18S).....	12

Online Safety Policy

Scope of the Policy

The regulation and use of technical solutions to safeguard learners are important but must be balanced with teaching the necessary skills to enable learners to take responsibility for their own safety in an ever-changing digital world. We aim to ensure that learners are able to use technology safely, respectfully, and responsibly. This includes keeping personal information private, maintaining a positive online footprint, recognising unacceptable behaviours and understanding a range of ways to report concerns about content and contact. Halton Adult Learning has a zero tolerance approach to online sexual abuse and/or harassment including (not limited to) sharing of explicit content, sexual coercion and sexualised comments or messages.

Learner safety is paramount and help, guidance and support will be available through the whole curriculum to enable them to recognise and avoid online risks and to build their resilience. During the delivery of the curriculum, staff will reinforce and consolidate safe online learning messages. Learners are encouraged to ask for help when they need it and report any concerns without delay.

This policy applies to all members of Adult Learning Service who have access to and are users of corporate ICT systems and online resources, both in physical and online learning environments.

The service will deal with incidents as outlined within this policy, within the remit of their safeguarding, behaviour and acceptable use policies (and others when applicable). Records will be kept to identify patterns and to intervene early to prevent abuse.

Monitoring and Review

The implementation of this Online Safety Policy will be monitored by:

- Adult Learning and Skills Manager
- Quality and Learner Experience Manager
- Divisional Manager

The service will monitor the impact of the policy using:

- Logs of reported incidents

- Monitoring logs of internet activity (including sites visited) via Smoothwall daily report
- Internal monitoring data e.g. LID activity, Learner Voice, team meetings

Divisional Management Group will be updated on the implementation of the Online Safety Policy at regular intervals, notably at monthly DMG meetings. Should serious online incidents take place, the relevant external persons / agencies should be informed as appropriate e.g. Police, Social Services. In the event of serious or repeated incidents, a full report will be presented to the Adult Learning Governance Group for scrutiny.

Roles and Responsibilities

Management Team

The Management Team, consisting of Divisional Manager, Adult Learning and Skills Manager and Quality and Learner Experience Manager are responsible for ensuring the day-to-day safety (including Online) of all learners. They will ensure that:

- all members of the service understand and acknowledge their responsibilities in the event of a serious online allegation being made (Appendix 1)
- all relevant staff receive suitable training to enable them to carry out their safeguarding responsibilities within the remit of the Online Safety Policy
- up to date Online Safety information is regularly communicated and promoted

The Safeguarding Lead

The Designated Safeguarding Lead will:

- ensure that the Online Safety Policy is accessible to all Adult Learning staff via SharePoint
- examine regular monitoring reports generated from the Smoothwall

The Safeguarding Lead is also responsible for taking any necessary action as per the Online Safety Incident reporting flowchart (Appendix 1). They will be trained in online issues and acknowledge and understand the potential for safeguarding issues that arise from, but not limited to

- sharing of personal data

- accessing illegal / inappropriate materials
- potential or actual incidents of radicalisation
- cyber-bullying

Disciplinary procedures, as outlined in the Learner Disciplinary Flowchart, will be implemented in the event of inappropriate online behaviour e.g. bullying or harassment.

Governors

The Governing board will receive information about online incidents and monitoring reports as part of the regular Safeguarding updates. In response to any concerns raised, Governors review this Online Safety Policy in terms of its effectiveness.

Halton Borough Council ICT Team

The HBC ICT Team is responsible for the maintenance of the Smoothwall web filtering system and the generation/distribution of daily monitoring reports to the Designated Safeguarding Lead.

Adult Learning Staff

It is essential that all staff

- understand and acknowledge their responsibilities as outlined in this Policy
- have read and understood the Acceptable Use Policy
- keep up to date with the Online Safety Policy as part of their CPD
- have an up-to-date awareness of online matters pertinent to their learners
- report concerns and log incidents through the Safeguarding Process
- refer to Appendix 1 when addressing any suspected misuse or Online Safety Issue
- ensure that all digital communications are on a professional level and only carried out using approved systems
- apply this Online Safety Policy to all aspects of the Curriculum

- share, discuss and ensure that learners understand and acknowledge their responsibility to follow the Acceptable Use Policy as outlined in the Learner Information Pack
- are good role models in their use of all digital technologies
- are vigilant in monitoring how learners use digital technologies and access online content whilst in class

It is accepted that from time to time, for purposeful/appropriate educational reasons, learners may need to research topics (e.g. racism, mental health, and discrimination) that might result in internet searches being blocked. In such a situation, staff can request that the ICT helpdesk remove those sites from the filtered list. Any request to do so should be made via email with clear reasons for the need.

Technical support

The service's technical infrastructure is secure and actively reduces the risk of misuse or malicious attack. HBC ICT services will ensure:

- detected risks and/or misuse is reported to the Adult Learning Safeguarding Lead
- all learners are assigned an individual username and password
- internet access is filtered for all users. Illegal content is filtered by the broadband or filtering provider.
- 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
- 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 service systems and data. These are tested regularly and the infrastructure and individual workstations are protected by up to date virus software.

Learners

It is essential that all learners should:

- understand, acknowledge and adhere to the Acceptable Use Policy
- be able to recognise inappropriate content or behaviours and know how to report it e.g. relating to radicalisation or sexualised content
- accept their responsibility to respond accordingly to any content they consider as inappropriate
- understand the importance of being a responsible digital citizen and maintaining a positive online footprint
- know that any breach of the Online Safety Policy will be dealt with in accordance with the Learner Disciplinary Policy and Procedure

The Adult Learning Service will provide online safety information and awareness through, but not limited to:

- newsletters, website links, social media channels
- learner workshops/classroom activities
- promotional campaigns e.g. Safer Internet Day

Useful Information

Safeguarding

In the event of a Safeguarding infringement or suspicion, procedure outline in Appendix 1 must be followed with consideration of the following:

- Record details of any website containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary for the Safeguarding officer to record and store screenshots of the content. These may be printed and signed (except in the case of images of child sexual abuse – see below)
- For adult learners, if content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the police would include: incidents of ‘grooming’ behaviour (including radicalisation), the sending of obscene materials to a child, adult material which potentially breaches the Obscene Publications Act, criminally racist material, other criminal conduct, activity or materials. Isolate the

computer in question as best you can. Any change to its state may hinder a later police investigation*

- Where explicit images are created/shared/stored between users aged under 18, the primary concern should be the welfare and protection of any young people involved. Incidents should be reported to the Safeguarding Lead Officer immediately and will be risk assessed (Questions to support assessment: Appendix 2) based on case context and risk of harm. Parents/carers will be informed unless there is reason to believe that this would put the young person at risk of harm. A referral will be made to children's social care and/or the police immediately if there is a concern that a young person has been harmed or is at risk of immediate harm at any point in the process.
- Where a safeguarding concern regarding an adult at risk is raised, safeguarding procedures as outlined in the Adult Learning Safeguarding Policy (including Prevent) should be followed.

*It is important that all of the above steps are taken as they will provide an evidence trail and demonstrate that visits to these sites were carried out for safeguarding purposes.

Data Protection

Personal and sensitive data will be recorded, processed, transferred and made available according to the Data Protection Act 2018. For further information please refer to Corporate Information Governance Handbook.

Communications

When using communication technologies the service considers the following as good practice:

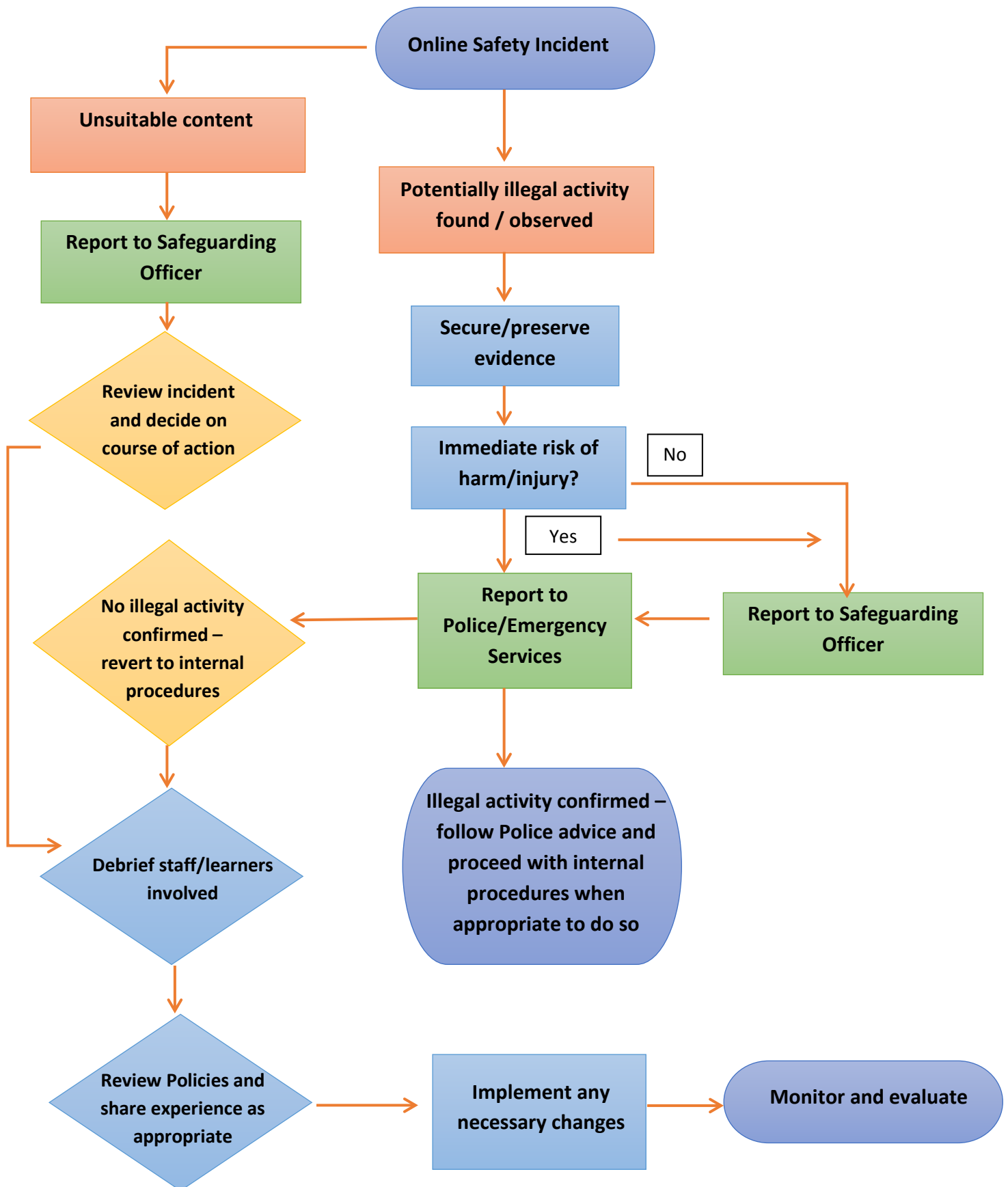
- The Outlook email service is safe and secure and is monitored. Users should be aware that email communications are monitored.
- When accessing emails off site, staff will only be able to access their corporate emails using Google Authentication app.

- Users must immediately report to their tutor/line manager the receipt of any communication that makes them feel uncomfortable, is offensive, sexual, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff and learners (email, chat) must be professional in tone and content. Personal email addresses, text messaging or social media must not be used for these communications.
- Learners should be taught about online issues, such as the risks attached to the sharing of personal details. They should also be reminded of the need to communicate appropriately when using digital technologies and the potential impact of a poor digital footprint, on employment prospects for example.
- Personal information should not be posted on the Adult Learning website and only official email addresses should be used to identify members of staff.

Social Media

The service's use of social media is to promote the ethos of the service. It is the responsibility of all staff to ensure that the content they upload is for professional purposes only and is compliant with Halton Adult Learning's values and aims. All Social Media accounts will be password protected and will be monitored and managed by appointed Learner Services Officer. Any inappropriate posts will be removed immediately.

Appendix 1 - Online Safety Incident Flowchart



Appendix 2: Questions to support assessment (Under 18s)

When deciding whether to involve the police and or children's social care in sharing of explicit images between persons under the age of 18, consideration should be given to the following questions.

Do you have any concerns about the young person's vulnerability?

Consideration should be given to whether a young person's circumstances, background or sexuality makes them additionally vulnerable and should be referred to children's social care. This could include:

- being in care
- having special educational needs or disability
- having been a victim of abuse
- having less direct contact with parents
- lacking positive role modelling at home

Why were the nudes and semi-nudes shared? Was the young person put under pressure or coerced or was consent freely given?

Young people's motivations for sharing nudes and semi-nudes include flirting, developing trust in a romantic relationship, seeking attention or as a joke.

A referral should be made to the police if a young person has been pressured or coerced into sharing an image, or images have been shared without consent and with malicious intent. Consideration should also be given to a young person's level of maturity and the impact of any special educational needs or disability on their understanding of the situation.

Action should be taken, in accordance with the setting's behaviour policy, with any young person who has pressured or coerced others into sharing nudes and semi-nudes. If this is part of pattern of behaviour then a referral to a Harmful Sexual Behaviour service should be considered, such as the National Clinical Assessment and Treatment Service (an NSPCC service).

Have the nudes and semi-nudes been shared beyond its intended recipient? Was it shared without the consent of the young person who produced the images?

The nudes and semi-nudes may have been shared initially with consent but then passed on to others. A young person may have shared them further with malicious intent, or they may not have had a full understanding of the potential consequences. Consideration should again be given to the level of maturity and the impact of any special educational needs on their understanding of the situation.

The police should be informed if there was a deliberate intent to cause harm by sharing the nudes and semi-nudes or if they have been used to bully or blackmail a young person.

Did the young person send nudes and semi-nudes to more than one person?

If a young person is sharing nudes or semi-nudes with multiple people, this may indicate that there are other issues which they need support with such as self-esteem and low confidence or harmful sexual behaviour. Consideration should be given to their motivations for sharing. A referral to children's social care should be made if there are wider safeguarding concerns.

Does the young person understand the possible implications of sharing the nudes and semi-nudes?

Young people may produce or share nudes and semi-nudes without fully understanding the consequences of what they are doing. They may not, for example, understand how it may put them at risk or cause harm and may not understand consent. Exploring their understanding can help assess whether the young person passed on an image with deliberate intent to harm and plan an appropriate response.

Are there additional concerns if the parents or carers are informed?

Parents or carers should be informed of incidents of this nature unless there is good reason to believe that informing them will put the young person at risk. This may be due to concerns about parental abuse or cultural or religious factors which would affect how they or their community would respond. If a young person highlights concerns about involvement of their parents or carers, then the DSL (or equivalent) should use their professional judgment about whether it is appropriate to involve them and at what stage. If the education setting chooses not to involve a parent or carer they must clearly record the reasons for not doing so. Where possible, children and young people should be supported to speak with their parents or carers themselves about the concerns.