Hampshire Achieves
Participation & Lifelong Learning

Hampshire Achieves
&
Secure & Specialist

Internet & e-Safety Policy & Procedures

Date of last review/update	February 2023
Review Frequency	Biennially
Reviewers:	Wendy Scott Laura Hamson Kevin Rhodes

Hampshire County Council

Contents

Internet & e-Safety
The contents of this policy are an integral part of the service's Quality Assurance Frameworks.

1.0 Introduction
This Policy covers two Services in Participation and Lifelong Learning; Hampshire Achieves (HA) and Secure & Specialist Education.

HA is a curriculum delivery team which provides a range of directly delivered and sub-contracted learning programmes, including Apprenticeships, Programmes for Young People; Pathways and Supported Internships and Adult Learning Programmes (Adult & Community Learning (ACL) and Multiply) at different venues across the county.

Secure & Specialist Education is a curriculum delivery team who provide all of the education and enrichment provision in Secure and Specialist (S&S) settings across the county. There is also a hybrid tutoring provision provided for the county, accessed by Hampshire County Council teams and schools.

2.0 Purpose
The Services aim to provide a safe and secure learning environment for all staff and learners. "A Safe Space is a place or environment in which a person or category of people can feel confident that they will not be exposed to discrimination, criticism, harassment or any other emotional or physical harm." (Oxford Dictionary)

The Services are committed to ensuring that a consistent approach is adopted in respect of internet and e-safety for all staff and learners across its settings and provision, regardless if these are delivered directly by HA or by one of its sub-contracted Learning Providers.

3.0 Scope
The primary duty of care in respect of the safety of staff and learners whilst using the Internet and e-technologies is the responsibility of; HA through its curriculum team delivering on internal Adult, Young People's Learning and Apprenticeship.

Learning Providers subcontracted by HA to deliver any form of education have the primary duty of care for these learners' safety in terms of using Internet and e-technologies.

The primary duty of care in respect to staff and learner safety when using the Internet and e-technologies is the responsibility of Secure and Specialist Education during the hours of education and by Southern Health and Swanwick Lodge Care Team outside of education hours.

Both Services will work in partnership with all relevant stakeholders and Learning Providers to promote and secure the concept of the "safe learner" in respect of internet and e-safety safety.

3.1 Related Policies
This policy is developed in the context of other related policies, including:
Hampshire Achieves Safeguarding and Prevent Policy

4.0 Implementation

HA will ensure that the safety of staff and learners whilst using the Internet will be facilitated by the relevant curriculum team or Learning Provider.

All teams and Learning Providers will take such precautions as are reasonably practical to provide and maintain safe and healthy working/learning conditions for staff and learners.

This will include:

- checking settings of any platforms being used to limit any potential harm;
- ensuring all are informed and aware of what behaviour is and isn't appropriate;
- having clear protocols in place for responding to any concerns;
- making sure learners know how to raise concerns and seek support if required;
- passing any concerns raised onto the appropriate person or agency in a timely manner.

The use of the Internet, email and other e-technologies by staff and learners is permitted and encouraged, and where such use supports the goals and objectives of the learning programme.

All Learning Providers will have their own internet safety policy, and this should include practical steps that will achieve the objectives of this policy by providing and maintaining high standards of safety for staff and learners, as far as is reasonably practicable.

The inclusion of an internet safety element in all relevant HA contract documents, places the primary duty of care with the Learning Provider.

The Learning Provider will:

- do everything possible to ensure that hardware, software and networks are safe and secure, for example using two factor identification, filtering, encryption, firewalls and anti-virus software;
- assess their use of technology for risks to staff, learners and information security. The assessment should be recorded and include any actions taken to mitigate any risks, including the risk of learners accessing websites linked to radicalisation and extremism.
- ensure that all users of technology abide by the Councils and/or their Learning Providers Acceptable Use Policy/Statement - see Appendix 1;
- provide support to staff and learners where necessary to ensure that they understand their responsibilities according to the Councils and/or their Learning Providers Acceptable Use Policy/Statement;
- deal with any breach of the acceptable use statement or policy in a timely manner, including, if necessary, referring to the Safeguarding and Prevent policy, or reporting to the police in the case of illegal activity.

5.0 Communications

We recognise that the use of e-technologies for communication can greatly enhance the learning experience. Therefore, all curriculum teams and Learning Providers should:

- consider carefully which modes of communication will be useful to them;

- give guidance to learners to ensure that they know how to use communication technology, including social media, in a way which is safe and prevents radicalisation and extremism and any form of harassment and/or bullying.

5.1 Delivering learning via online platforms

The use of online delivery applications and recordings can be very beneficial to learning, teaching and assessment. However, the associated risks should be carefully managed. The Services need to ensure the safeguarding of both our staff and learners when using online classrooms.

HA Apprenticeship Learners

All Hampshire County Council Corporate apprentices will be asked to complete the corporate Cyber Security – how to stay safe online via the Learning Zone. All other apprentices complete comprehensive Safeguarding modules as part of their learning, and the safeguarding unit is one of the first modules they complete.

Business Administration apprentices have been asked to complete 'Online Safety' and 'What can you trust' on https://www.et-foundation.co.uk/news/side-side-learner-prevent-duty-online-modules, apprentices have also been asked to feedback on the suitability of modules once completed.

All apprentices will have access to MS Teams and will complete the MS Teams – 'Getting started' and 'MS Teams Calls' online learning activity again through the Learning Zone.

All learners will also be asked to complete and sign a multimedia consent via the enrolment form and will be advised when online delivered sessions may be recorded, including the issuing of a privacy statement (see appendix 5).

As good practice, all tutors at the start of each session are to remind learners that the sessions are being recorded, and that any audio, video image or comments made within the group chat will be recorded and viewable by others.

HA Young Peoples Learning Learners

These learners will be complete the Education and Training Foundation Side by Side course modules on:

- Online Safety
- What can you trust?

Learners must complete and sign a multimedia consent as part of the enrolment process, and where necessary the parents/carers and/or guardians of learners, must also be made aware that the online sessions may be recorded.

Secure and Specialist Education

All learners who join the Secure and Specialist settings have an account created for them on a site-based closed network. This enables all access to be monitored or where required, restricted. It also means that all usage can be reviewed, including sent emails.

Prior to using any facilities, permissions have to be secured either by parents, the wider Multi-Disciplinary Team or from The Ministry of Justice dependent on the restrictions placed on the individual. All learners have an introductory session which explores the facilities and covers both operational and safety aspects of the tools in use. This session also makes

clear the monitoring systems in place and requires learner to agree to adhere by the guidance.

In physical settings, full staff supervision is in place at all times. Where there is any information technology usage this staff supervision is used to ensure usage is appropriate but that any restrictions placed on the learner are maintained. This means that staff will position themselves with a clear view of the screen.

All online resources are reviewed and evaluated by staff prior to use, to ensure suitability. The site-based network also features a firewall which meets the requirements for Hampshire Schools. Networks and permissions can be implemented by staff on site, in order to ensure all, remain current and appropriate. Any misuse use of the technology is considered a safeguarding breach and therefore is reported to both the HA DSL and relevant partner agencies.

Ongoing e-safety learning is provided through PSHE and digital skills sessions, which are integral parts of the Character Curriculum in all areas.

HA Adult and Community Learning
Learners attending adult and community learning courses delivered online must be given safeguarding advice on how to stay safe online by their Learning Provider.

All learners are asked to complete and sign the multimedia consent section within the online enrolment forms.

Providers may choose to ask learners to complete 'Online Safety' and 'What can you trust' on https://www.et-foundation.co.uk/news/side-side-learner-prevent-duty-online-modules/, or may investigate more age appropriate resources.

HA is unable to endorse any specific online delivery software. Therefore, Learning Providers should take careful consideration on the platforms they use and how the safety and security of both tutors and learners is maintained.

Online delivery tutors advise learners at the start of each session if the session they are attending is being recorded, and if so, that any comments made within the group chat will be saved and viewable by others.

Other essential points to ensure:

- Classes are delivered in 'closed' mode so that only invited learners can participate;
- Clear guidelines are issued to learners on contact and interaction with other learners on the course;
- Boundaries are set regarding online behaviours.

5.2 Use of recordings – audio/images/video

The use of recordings can be very beneficial to learning, teaching and assessment and the associated risks should be carefully managed. Providers will:

- ensure that permission is sought to use recordings of learners and staff/volunteers see appendix 5 privacy notice;

- carefully assess the use of recordings of any type when sharing or distributing online to ensure that the use does not place any individual in a vulnerable position or go beyond permissions granted by individuals.

5.3 Social media

When thinking about using social networking, a common-sense approach should be taken. Safeguarding principles and basic manners in how we communicate with people must be adhered to. If it is right and proper to be courteous, discrete, and professional when communicating with people in person (inside or outside of the organisation) then the same rules should apply when typing anything into a computer or a communication device. Likewise, if the rules to keep young people and adults safe and the sharing of information protocols within the organisation are important when dealing face to face with people, the same principles should again apply when posting anything onto the World Wide Web.

Social networking websites and applications include, but are not limited to:

- Snapchat
- Facebook
- You Tube
- Instagram
- WhatsApp
- Twitter
- Online forums

All these sites allow individuals and groups to communicate using a variety of communication methods. Learners will be able to use social media sites/apps within a learning environment in accordance with their tutor's instruction, as long as it is part of their course.

Befriending: One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. Staff should maintain a boundary between their professional and personal lives and should not accept personal invitations to "friend" learners (children or young people) or initiate personal friendships with learners, or learners' family members/friends.

Security: Learners and staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly. Even with privacy settings in place it is still possible that the personal details of learners and staff may be accessed more broadly than the other networkers identified by them. In using social networking sites, learners and staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site, it may remain available and accessible.

Where learners personal mobile telephone numbers are used such as with WhatsApp, learners should agree to only use these accounts for course-based discussions. Staff are requested to use work mobiles and/or create separate email accounts to use for **their** professional role. Staff should not create/use platforms with personal accounts/mobile numbers, if needed they should create a separate professional account for use within their tutoring role.

6.0 Training for staff

The Services and its sub-contracted providers will ensure that staff and volunteers receive information and training, as appropriate, to ensure that they:

- understand internet and e-safety issues and risks;
- abide by the Councils and/or their Learning Providers Acceptable Use Policy/Statement;
- are aware of where to go to get help and advice;
- are aware of the reporting procedures;
- embed e-safety, as appropriate, in their teaching practice;
- can access relevant e-learning resources on e-safety and the Prevent Duty from for example Get Safe Online | Free, online security advice and the Education and Training Foundation;
- Ensure their Safeguarding (including Prevent) training is up to date.

7.0 Safeguarding

All staff should follow these generic protocols when using the online delivery applications to ensure the safety of themselves and the learners.

- Ensure that permission is sought to use recordings of learners and staff – see updated multimedia consent form;
- Carefully assess the use of recordings of any type when sharing or distributing online to ensure that the use does not place any individual in a vulnerable position or go beyond permissions granted by individuals;
- Professional accounts: do not create/use platforms with personal accounts, if needed create a separate email account to use for your professional role;
- If creating a video or live stream, consider your background. This should be neutral with no personal photos or likelihood of other people being seen/identified;
- Consider background noise e.g., conversations that might be overheard, music and TV;
- Ensure groups are closed groups.
- Consider how input from others is controlled e.g., ensure that there is option for learners to opt out of video (camera off), tutor to control who has open mic;
- Identify to learners if the session will be recorded;
- Ensure the tutor has full control of who is allowed to present/share screen;
- Be mindful that some learners may not wish to turn on their video on, on a particular day/days/session;
- It is good practice to have a moderator (additional Tutor, LSA or Skills Coach) to support delivery of the chat to ensure comments are appropriate and questions flagged to the tutor. Attire should be the same as when you teach face to face – smart and professional.

8.0 Reporting Procedure

The Services and its sub-contracted Learning Providers will:

- advise learners to report any e-safety incident, including those related to radicalisation and extremism to their tutor or other members of the provider staff
- advise staff to report any e-safety incident, including those related to radicalisation and extremism to their line manager

- advise staff if they become aware that a learner (or group of learners) has made inappropriate/insulting/threatening comments about another learner or a member of staff on a social networking site; they must report this to their line manager so that the appropriate action can be taken
- record any incidents and the course of action taken to remedy the situation.

Where the misuse presents a safeguarding concern, HA Designated Safeguarding Lead/Officer should be informed.

9.0 Monitoring, Review & Audit

The contents of policy will be monitored regularly by Hampshire Achieves Performance Management Group (PMG). Policies and procedures will be kept updated in accordance with any mid-year changes in the law, regulations, or changes to the Services' provision, with updates approved by PMG. All policy and procedures will be reviewed by Senior Managers to determine their effectiveness, and where any changes are required, these will be applied and ratified. A summary of all changes will be kept as part of the PMG meeting notes. In addition, a cycle of internal policy compliance/audits defined by Senior Managers will provide the assurance of the overall effectiveness of the Services ethos, policies, and procedures, and will confirm operational effectiveness, and compliance with our own quality assurance framework and any relevant laws or regulations.

Appendix 1 Acceptable Use Statement
(also included in all HA learner handbooks)

Use of the Internet and email by learners is permitted and encouraged where such use supports the goals and objectives of the learning programme.

HA has a policy for the use of the Internet and email whereby learners must ensure that they:

- follow any given guidelines to stay safe online
- comply with current legislation
- use internet and email in an acceptable way
- do not create unnecessary business risk to HA, or to their Learning Provider, by their misuse of the internet/email.

Unacceptable behaviour

The following behaviour by a learner is considered unacceptable:

- use of HA or Providers communications systems to set up personal businesses or send chain letters
- distributing, disseminating or storing images, text or materials that might be considered indecent, pornographic, obscene or illegal
- distributing, disseminating or storing images, text or materials that might be considered discriminatory, offensive or abusive, in that the context is a personal attack, sexist or racist, or might be considered as harassment
- accessing copyrighted information in a way that violates the copyright
- broadcasting unsolicited personal views on social, political, religious, or other non-business-related matters
- transmitting unsolicited commercial or advertising material
- introducing any form of computer virus or malware into the corporate network.

Appendix 2 Multimedia Consent form

(to be completed by all learners completing a paper-based enrolment form)

Name:

Address: ……

Contact telephone number: .....

Learning programme:.....

Venue or location of photoshoot: .....

Hampshire County Council would like to take photographs, audio, and/or make a video recording of you for promotional and educational purposes.

Photograph and/or film may appear in printed and electronic publications, newsletters, in media releases, on our website, on social media sites e.g., Twitter and Facebook, on our Moodle virtual learning environment or other teaching platforms such as Adobe Connect, MS Education and Zoom or on all or any combination of these platforms.

To comply with data protection legislation, we need your permission before we publish or share any photographs or recordings of you.

Please read **all** sections of this form and confirm your consent by signing and dating the form on the next page where shown.

The information you provide (address, contact numbers) will be securely stored and processed within the European Economic Area and not be used for any other purpose than confirming your permission to use the material.

For further information about your data protection rights, please see the Hampshire County Council Privacy Notice at https://www.hants.gov.uk/aboutthecouncil/privacy

Conditions of use *(please delete as appropriate)*

Photographic Images, Audio or Video Recordings

HCC Website	**Yes / No**
Publications / Newsletters	**Yes / No**
Media releases	**Yes / No**
Hampshire Achieves VLE	**Yes / No**
Teaching platforms such as Adobe Connect, MS Education and Zoom	**Yes / No**
Social Media e.g. Twitter or Facebook	**Yes / No**

- This form is valid for seven years from the date of signing.
- After this time your consent will expire, and your images and personal data will be deleted from our records.
- We will not include details or full names (which means first name and surname) of any person in an image/recording without seeking further consent.
- Your consent can be withdrawn in writing at any time by emailing participation.lifelong.learning@hants.gov.uk
- When images are uploaded to social media sites, they will be subject to the terms and conditions of those sites.
- Please note that websites and social media sites can be seen throughout the world and not just in the United Kingdom where UK law applies. Neither you nor the County Council will have control over how those images are further used.

~~~~~~

Consent

I have read and understood the conditions of use and give my consent for my image(s), film(s) and/or audio recordings to be used as described above.

Your signature: ……………………………………… **Date:** …………………………

Your name (in block capitals): …………………………………………………………

Please return your completed signed form (electronic or Paper-based to your course tutor).
~~~~~~

Appendix 3 Links to useful websites

www.thinkuknow.co.uk
www.digizen.org
www.childnet.com
www.ceop.gov.uk
www.facebook.com/safety
www.getsafeonline.org
www.saferinternet.org.uk/
https://learning.nspcc.org.uk/research-resources/schools/safer-internet-resources
www.internetmatters.org/
www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis

The VLE has a wide range of information on how to set up and use software such as MS Teams, as well as advice and guidance on best practice for online delivery with a variety of webinars. *One key element of successful online delivery is making sure you are familiar with the software and the tools available. Please use these resources to check that you have considered all elements of delivery, including security, inclusion, accessibility, and engagement.*

Appendix 4 Learners to consider:

Location

- When joining a class/session they should choose an appropriate place. This needs to be somewhere quiet where they are able to focus.
- If you are using a video interaction/webcam, then bedrooms are not always considered suitable places. If this is the only option for learners, then they should have a neutral background or virtual background.

Behaviour

- Language and behaviour should be the same level as if they were in an actual classroom.

Privacy

- Consider the privacy of others in their household and ensure if they are using video/webcam that others are not visible and avoid backgrounds that show personal items e.g., photos. Some platforms allow you to blur your background.

Dress and attire

- Dress as they would in a classroom – no pyjamas. This helps create a professional mindset and helps to create a focused time.

Safety

- having a separate email account that is used for their learning. This will ensure their other personal accounts are secure, and if they wish to leave the group, or restrict access to their learning they have more control.

Appendix 5 Privacy notice for Teams recordings

Recording on Microsoft Teams Privacy Notice

Why do we collect and use this information?
Hampshire County Council is the Data Controller for the purpose of collecting and using information from meetings, training and other scheduled activity, being hosted through the Microsoft Teams software within the County Council's O365 suite of tools.

Through the recording of the session, we are collecting information from participants attending virtually or in person, through the system's video, audio and chat functions; and hold this personal data securely and use it to:

- to provide an accessible record of the event for those in attendance and those unable to attend but wishing to access the content;
- monitor attendance and update individual's learning history and/or support individual's professional development;
- assist in the planning of future services and sessions/activity;
- influence future training and "lessons to be learnt" activity;
- undertake statistical analysis; and
- ensure compliance with our obligations under the accuracy principle of the General Data Protection Regulation (Article (5)(1)(d)), making sure our records are up to date.

Microsoft is a data processor for this information acting on our instructions for the purpose of delivering a contract to the County Council around the supporting of the O365 suite of tools, which the County Council uses to collect and store the information provided to us, as identified under this privacy notice. This includes accessing the O365 Suite to fix any technical issues to ensure the system is fit for use.

The following sections provide further detail around the information we process setting out what allows us to do this (lawful basis), who we may share it with, how long we keep it for (the retention period), alongside identifying any rights you may have and who to contact if you think we're not handling your information in the right way.

The categories of information that we collect, hold and share
The following personal and special category information may be processed in undertaking this activity:

- attendee personal information (such as name, email address, department);
- information you have contributed to the session such as contributions in the chat function or questions asked during the session (please note the Q & A section of the session will not be recorded).

The lawful basis on which we use this information
We collect and use the information ensuring that we comply with the General Data Protection Regulation (GDPR) and the Data Protection Act 2018 (DPA2018) requirements for processing through:

- Article 6(1)(f) – the processing is necessary for the purpose of our legitimate interests. A legitimate interest test has been conducted to ensure that this processing does not override your interests or fundamental rights as a data subject.

Under this lawful basis we do not require consent to process information in this way, but we are required, through this privacy notice, to ensure you are fully informed of why we are collecting this information and what we will do with it. Please note that no automated decision making (decisions taken without a person involved) occurs for any parts of these activities controlled by the County Council. The County Council does not use profiling for this service.

Storing and Securing Data
The information provided to us will be recorded and stored within the County Council's Document Management System (DMS), The information held within the County Council's DMS will be kept for in line with our retention schedule and then deleted as appropriate. The County Council's DMS is hosted by the County Council in secure UK based data centres, which are on site. No information leaves the European Economic Area (EEA).

The County Council takes its data security responsibilities seriously and has policies and procedures in place to ensure the personal data held is:

- prevented from being accidentally or deliberately compromised;
- accessed, altered, disclosed or deleted only by those authorised to do so;
- accurate and complete in relation to why we are processing it;
- continually accessible and usable with daily backups; and
- protected by levels of security 'appropriate' to the risks presented by our processing.

The County Council also ensures its IT Department is certified to the internationally recognised standard for information security management, ISO27001.

Who do we share information with?
We do not share information with anyone unless there is a lawful basis that allows us to do so. Information recorded in this session will be circulated to Children's Services staff only under the legitimate interest lawful basis as identified above. In addition to storage on SharePoint the recording will also be available on our VLE platform, within our staff training section.

Requesting access to your personal data and your rights
Under data protection legislation, individuals have the right to request access to information about them that we hold. To make a request for your personal information, or someone you have responsibility for, please contact the Children's Services Department's Subject Access Request (SAR) Team, whose contact details alongside further information around this process can be found via:
https://www.hants.gov.uk/socialcareandhealth/childrenandfamilies/accessrecords

You also have the right to:

- prevent processing for the purpose of direct marketing;
- object to decisions being taken by solely automated means;

- in certain circumstances, have inaccurate personal data rectified, blocked, erased or destroyed; and
- claim compensation for damages caused by a breach of the Data Protection regulations.

If you have a concern about the way we are collecting or using personal data, you can raise your concern with us in the first instance or you can go directly to the Information Commissioner's Office, as the supervisory authority, at https://ico.org.uk/concerns/.

Contact Details
For further information on how we handle personal information, individual's data rights, how to raise a concern about the way we are processing information and the County Council's Data Protection Officer, please see our General Privacy Notice: https://www.hants.gov.uk/aboutthecouncil/strategiesplansandpolicies/dataprotection