TITLE		REF	VERSION
Online Safety Policy		LS030	3.0
APPROVAL BODY:		**DATE**	**REVIEW DATE**
GET		6 October 2026	6 October 2027
LEAD PERSON	Director - Designated Safeguarding Lead		
EQIA DATE	August 2024	**DPIA DATE**	August 2024

ONLINE SAFETY POLICY

Contents

1. Policy statement
2. Commitment Statement
3. Purpose
4. Scope
5. Responsibilities
6. Systems for Online Safety
7. Responding to Incidents of Concern
8. Multimedia and Advance Technologies
9. Teaching and Learning
10. Review
11. References

1. Policy Statement

Activate Learning recognises that digital technology and online services are an integral to education, employment and everyday life. We are committed to ensuring that all members of our community can benefit from technology in a safe, supportive and inclusive way.

Online safety is a fundamental part of safeguarding and promoting the welfare of children, young people and adults at risk. We promote a positive culture in which students, apprentices, staff and partners are equipped to use technology safely, responsibly, respectfully and confidently, and are able to recognise and respond to online risks. Activate Learning recognises that the nature and level of online risk is not the same for every individual and may vary according to age, developmental

stage, learning context, digital independence, frequency and intensity of online activity, and individual circumstances.

This policy sets out Activate Learning's approach to online safety and our commitment to safeguarding our community in accordance with statutory guidance and recognised best practice, including *Keeping Children Safe in Education*, *Working Together to Safeguard Children*, the *Prevent Duty Guidance*, *Meeting Digital and Technology Standards in Schools and Colleges*, and other relevant guidance.

2. Purpose

The purpose of this policy is to embed online safety within Activate Learning's safeguarding arrangements and our culture of Safe Students, Safe Staff, Safe Spaces.

The policy:

- defines the roles and responsibilities of members of the Activate Learning community in promoting online safety;
- establishes expectations for the safe, secure and responsible use of digital technologies, devices, networks and online services;
- outlines how students and apprentices will develop the knowledge, critical thinking, resilience and skills needed to navigate online opportunities and risks;
- sets expectations for staff in their professional use of technology and digital communications;
- provides a framework for preventing, identifying, recording, responding to and managing online safety concerns and incidents;
- supports compliance with safeguarding requirements through appropriate filtering, monitoring and cyber security arrangements; and
- provides for the regular review of online safety arrangements in response to technological developments, emerging risks and organisational learning.

This policy should be read alongside other relevant Activate Learning policies and procedures, including the IT Services Acceptable Use Policy and Procedure, Safeguarding and Prevent Policy, Safeguarding – Reporting a Concern Procedure, Professional Conduct Policy, Social Media Policy, Artificial Intelligence Usage Policy, Information Security and Data Protection Policy and the Student Positive Behaviour Management Policy.

3. Commitment Statement

Activate Learning takes a whole-organisation approach to online safety and recognises that safeguarding in the digital environment is everyone's responsibility. In line with our Learning Philosophy and Trauma Informed Practice, we are committed to ensuring that students and apprentices can participate confidently in learning both online and offline, while staff model safe, professional and responsible digital behaviour.

Effective online safety requires collaboration across safeguarding, curriculum, student support services, IT Services, leadership, governors, employers, parents/carers and students and apprentices themselves. We will work collectively to promote positive and responsible use of technology, strengthen digital resilience, and ensure that concerns are recognised, reported and addressed appropriately.

We are committed to preventing and responding to online abuse, exploitation, harmful content and other emerging digital risks. This includes maintaining effective filtering, monitoring and cyber security arrangements that meet the Department for Education's Filtering and Monitoring Standards.

As technology and online behaviours continue to evolve, we will regularly review our systems, practices and educational provision to ensure that our online safety arrangements remain effective, proportionate and responsive to emerging risks.

4. Scope

This policy applies to all members of the Activate Learning community, including students, apprentices, staff, governors, volunteers, contractors, agency staff, visitors,

employers, partners, parents/carers and any other individual using or accessing Activate Learning digital systems, devices, networks or online services.

It applies to technology used:

- on college premises including in residential accommodation;
- during work placements and apprenticeships, where relevant;
- whilst working or learning remotely;
- during live online teaching, virtual meetings and asynchronous learning;
- on college-owned or personal devices including Bring Your Own Device (BYOD); and
- in connection with Activate Learning activities.

Online safety concerns may arise on or off college premises and through technologies or platforms that are not owned or managed by Activate Learning. Where behaviour outside the organisation presents a safeguarding risk to a student, apprentice, member of staff or the wider college community, Activate Learning will respond in accordance with this policy and the Safeguarding and Prevent Policy.

Where appropriate, concerns will be shared with parents/carers, employers, partner organisations or external agencies in accordance with safeguarding procedures, information-sharing requirements and applicable legislation.

5. Responsibilities

Creating and maintaining a safe online environment is a shared responsibility. All members of the Activate Learning community have a role in promoting the safe, responsible and appropriate use of technology.

5.1 Corporation Board

The Corporation Board has strategic oversight of online safety and safeguarding. The nominated Safeguarding Governor (including Online Safety and Residential Accommodation) receives regular assurance regarding the effectiveness of Activate Learning's online safety arrangements, including filtering and monitoring, emerging risks, incidents and compliance with statutory guidance.

5.2 Group Executive Team

The Chief Learning Officer (Curriculum) has executive oversight of safeguarding, including online safety, and chairs the Safeguarding Committee.

The Group Executive Team is responsible for:

- approving this policy and ensuring sufficient resources are available to implement it;
- ensuring online safety forms part of organisational risk management and safeguarding governance;
- receiving regular assurance on the effectiveness of online safety and cyber-security arrangements through audits, incident reporting and annual review, including use of the SWGfL 360-degree self-review tool.

5.3 Online Safety Lead

The Director – Designated Safeguarding Lead (DSL) is the organisational Online Safety Lead and works collaboratively with the Group Director of Institutional Effectiveness and IT Services.

The Online Safety Lead is responsible for:

- leading the organisation's strategic approach to online safety as part of safeguarding;
- ensuring compliance with statutory safeguarding guidance, including *Keeping Children Safe in Education*, DfE's *Meeting Digital and Technology Standards in Schools and Colleges,* and the *Prevent* Duty;
- ensure all staff undergo annual safeguarding training (including online safety) and share regular updates about online safety issues and trends;
- overseeing the response to online safeguarding concerns and ensuring appropriate recording, referrals and support;
- promoting online safety education through staff development, curriculum and awareness campaigns, and ensure that online safety education is embedded across the curriculum;

- working with technical staff to review filtering, monitoring and cyber security arrangements, at least annually;
- providing regular assurance and reporting to governors and senior leaders.

5.4 Designated Safeguarding Leads and Safeguarding Teams

The DSL, Deputy DSLs, Team Leads, and Safeguarding Teams receive appropriate online safety training and manage safeguarding concerns arising from online activity in accordance with Activate Learning's safeguarding procedures.

5.5 Group Director for Faculty and College

Group Directors are responsible for ensuring that online safety is embedded within curriculum delivery, student support and enrichment programmes, enabling students and apprentices to develop the knowledge, skills and resilience needed to stay safe online.

5.6 Staff

Online safety is everyone's responsibility.

All staff must:

- understand that online safety is an integral part of safeguarding;
- complete mandatory safeguarding and online safety training and keep their knowledge up to date;
- model safe, responsible and professional use of technology in line with the IT Acceptable Use Policy;
- use only Activate Learning-approved communication platforms, digital services and AI tools for work purposes, in line with the Professional Conduct Policy and Social Media Procedure;
- protect personal and organisational data in accordance with UK GDPR and organisational policies;
- critically review AI-generated content before use, recognising the potential for inaccuracies, bias and fabricated information;

- supervise students and apprentices appropriately when using digital technologies;
- identify, record and report online safety concerns promptly in accordance with the Safeguarding – Reporting a Concern procedure;
- promote respectful online behaviour and challenge bullying, discrimination, harassment, extremism and other harmful online conduct in line with the Student Positive Behaviour Management Policy.

5.7 IT Services and Technical Staff

Technical staff, supported by the organisation's IT provider, are responsible for maintaining a secure digital environment by:

- implementing and maintaining appropriate filtering and monitoring systems in line with the DfE Filtering and Monitoring Standards;
- ensuring networks, systems and devices are secure, controlled, and appropriately managed;
- supporting risk assessments, procurement and change management for digital systems;
- monitoring technical risks, sharing updates, and responding promptly to identified concerns;
- working closely with safeguarding staff to review the effectiveness of filtering and monitoring arrangements, conducting updates at least annually.

5.8 Students and Apprentices

Students and apprentices are expected to:

- use digital technologies safely, responsibly and in accordance with the IT Acceptable Use and Online Safety Policy;
- report online safety concerns, harmful content or inappropriate behaviours promptly;
- behave respectfully online and understand that online behaviours outside Activate Learning may still be addressed where it affects members of the college community;
- maintain appropriate professional boundaries when communicating with Activate Learning staff and must not use personal social media accounts or

social media messaging services to contact staff. Communication with staff should take place through approved Activate Learning communication channels;

- use AI and digital technologies ethically, respecting copyright, academic integrity and the work of others

5.9 Parents and Carers

Parents and carers are encouraged to support Activate Learning by reinforcing safe and responsible technology use, engaging with online safety information provided by the organisation and reporting concerns where appropriate.

5.10 Visitors, Contractors and Community Users

Anyone accessing Activate Learning's digital systems or networks must comply with relevant acceptable use requirements and act in accordance with this policy.

6. Online Safety Framework

6.1 Online Safety Governance

Activate Learning adopts a whole-organisation approach to online safety through effective leadership, governance, collaboration and continuous improvement.

The Online Safety Working Group, chaired by the Online Safety Lead (Director – DSL), meets termly and includes representatives from safeguarding, curriculum, IT services and other relevant departments. The group provides strategic oversight of the organisation's online safety arrangements and monitors their effectiveness in accordance with the Online Safety Working Group Terms of Reference.

The Working Group is responsible for:

- monitoring the implementation and effectiveness of this policy;
- reviewing the effectiveness of filtering and monitoring arrangements;
- evaluating online safety education and awareness for students, apprentices, staff and our wider communities;
- considering emerging technologies, risks, online harms and sector developments;

- consulting with students, apprentices, staff and other stakeholders to inform continuous improvement;
- monitoring progress against online safety action plans, including recommendations arising from the South-West Grid for Learning (SWGfL) 360-degree Safe self-review tool and other assurance activities.

Separate Artificial Intelligence (AI) governance arrangements oversee the safe, ethical and lawful use of AI across the organisation. These arrangements support compliance with relevant legislation, organisational policies and emerging best practice whilst ensuring that AI-related risks and opportunities are appropriately managed.

6.2 Risk Management

Activate Learning recognises that students and apprentices have different levels of online exposure, independence, digital maturity and safeguarding need. Online safety arrangements will therefore be proportionate to their age and developmental stage, including the additional needs of 14–16-year-olds, as well as their programme, circumstances and level of online engagement. This includes considering adult learners who may be at increased risk, the requirements of Higher Education and academic freedom, and those who study or work predominantly or wholly online and may have greater exposure to online risks and fewer opportunities for face-to-face safeguarding oversight. SEND, care experience, exploitation, discrimination, isolation, financial vulnerability and other factors that may increase online vulnerability will also be considered. Safeguarding education, supervision, support, risk assessment, parental/carer engagement and technical controls will be adapted accordingly, where proportionate.

Activate Learning maintains a proactive approach to identifying, assessing and managing online safety risks. Online safety risks are monitored through a range of governance and assurance activities, including:

- annual completion of the SWGfL 360 Safe self-review tool;
- annual reviews of filtering and monitoring arrangements in line with the Department for Education's Filtering and Monitoring Standards;

- monthly, weekly and daily reviews of filtering and monitoring reports and alerts;
- safeguarding audits and quality assurance activities, and lessons learned processes.

Findings are used to inform improvements to policy, procedures, staff training, technical controls and online safety education.

6.3 Cyber Security

Cyber security is an integral part of safeguarding and online safety. Activate Learning maintains proportionate technical and organisational measures to protect its networks, systems, users and information from cyber threats, including unauthorised access, malware, phishing, ransomware and data breaches.

The organisation maintains recognised cyber security standards, including Cyber Essentials and Cyber Essentials Plus certification. Cyber security arrangements are subject to continuous monitoring, independent assurance, regular testing and oversight through organisational governance and risk management processes.

All IT users share responsibility for maintaining cyber security by following organisational policies, reporting suspected cyber incidents promptly and remaining vigilant to potential online threats.

6.4 Acceptable Use

All users are expected to use Activate Learning's digital technologies safely, responsibly, lawfully and professionally in accordance with this policy and the IT Services Acceptable Use Policy.

Expectations are communicated through induction, mandatory staff training, the Student Code of Conduct, curriculum delivery, awareness campaigns, digital communications and engagement with parents and carers.

6.5 Filtering

Activate Learning implements appropriate filtering systems in accordance with the Department for Education's Filtering and Monitoring Standards and guidance published by the UK Safer Internet Centre.

Filtering arrangements:

- apply to organisational networks, devices and guest wireless services;
- provide differentiated user-level and role-appropriate filtering where required;
- are reviewed regularly, including at least annually, to reflect emerging risks, safeguarding trends, educational requirements and changes in technology;
- support teaching, learning and research whilst reducing access to illegal, harmful or inappropriate content; and
- are proportionate to the environment in which technology is being used, recognising that different settings may have different legitimate requirements.

Filtering is not necessarily uniform across all Activate Learning settings. For example, students living in halls of residence may require access to services such as gaming websites that could otherwise be restricted on college networks, where this is considered appropriate to the residential environment and supports a more home-like experience. Such differentiated access remains subject to appropriate safeguarding, monitoring and risk management arrangements.

Filtering decisions are made collaboratively by safeguarding and IT to ensure an appropriate balance between protecting users and enabling legitimate educational, residential or other organisational activity. Where access to restricted content is required for teaching, learning or research, requests will be assessed and managed through the IT Service Desk [internal staff use only].

Where Activate Learning utilises systems or networks managed by partner organisations, such as Oxford Brookes University at Harcourt Hill halls of residence, the organisation works collaboratively with those partners to ensure filtering arrangements appropriately support safeguarding responsibilities while reflecting the needs of the setting.

Staff should recognise that filtering arrangements may differ when users access external networks, including during educational visits, work placements or university settings, and should take appropriate steps to assess and manage any associated risks.

6.6 Monitoring

Activate Learning recognises that filtering and monitoring are important safeguarding measures but do not replace effective supervision, professional curiosity, education or a strong safeguarding culture.

Appropriate monitoring is used to identify potential safeguarding concerns, inappropriate use of technology and threats to organisational systems. Alerts are reviewed by appropriately trained safeguarding, Human Resources and IT staff, with concerns managed proportionately in accordance with relevant procedures.

Monitoring arrangements support Activate Learning to:

- identify safeguarding concerns at the earliest opportunity;
- enable timely intervention where individuals may be at risk or pose a risk to themselves or others;
- detect misuse of organisational systems and malicious activity; and
- inform the ongoing review of filtering, safeguarding practice and online safety education.

Where internet use is planned, staff should direct students and apprentices to appropriate sites and ensure arrangements are in place to respond to unsuitable content identified through searches.

Staff should report to IT Services via the Service Desk where they:

- access or suspect that unsuitable material has been accessed using organisational systems;
- identify content that should reasonably be restricted;
- identify failures or concerns with filtering or monitoring;
- experience restrictions that unreasonably affect legitimate teaching, learning or business activity; or
- identify attempts to circumvent filtering, including through alternative spellings, abbreviations or other methods.

Where sensitive online content is required for legitimate teaching, learning or research, such as research into illicit substances within Health and Social Care or Nursing programmes, staff should notify IT Services and the Safeguarding Team in advance. This enables appropriate arrangements to be considered and avoids unnecessary safeguarding alerts or interventions.

6.7 Supporting Vulnerable Students

Activate Learning recognises that some students and apprentices may be at increased risk of online harm due to their individual circumstances, including those with SEND, care experience, adults at risk, and those experiencing discrimination or exploitation.

Where appropriate, online safety education, safeguarding support, risk assessments and technical controls will be adapted to individual needs to promote digital resilience and reduce barriers to staying safe online.

7. Safe Use of Technology

7.1 Device Management

Activate Learning supports the appropriate use of digital and mobile technologies, including organisation-owned and personal devices, to enhance learning, collaboration and digital skills.

All users must use devices safely, responsibly and respectfully, in accordance with this policy, the IT Services Acceptable Use Policy and other relevant procedures. Technology must not disrupt learning, work or the experience of others, and users must:

- comply with organisational security, filtering and monitoring arrangements;
- connect to organisational networks only through approved arrangements; and
- protect personal information, organisational data and the security of organisational systems.

Personal devices using mobile data or external networks are not subject to Activate Learning's filtering and monitoring. Users should therefore exercise appropriate judgement and remain alert to online safety risks.

Activate Learning may search, restrict or remove access to a device where there are reasonable grounds to believe it has been used to commit an offence, place someone at risk of harm or breach organisational policies. Organisation-owned devices may be audited or recalled in accordance with the IT Services Acceptable Use Policy. Personal devices are used on Activate Learning premises or during organisation-led activities at the owner's risk.

Students aged 14–16 are subject to additional expectations regarding mobile phones and personal devices. Wherever possible, these should not be used during taught sessions unless authorised for learning. Staff should reinforce responsible technology use through supervision and curriculum delivery, including online safety, digital citizenship and social media education.

Where device use disrupts learning, compromises safeguarding or breaches organisational expectations, staff may instruct a student to put the device away or surrender it and may take further action in accordance with the Student Positive Behaviour Management Policy and, where necessary, the Student Search Procedure.

7.2 Generative Artificial Intelligence (AI)

Activate Learning recognises the educational and business benefits of generative AI while recognising the associated safeguarding, ethical, privacy and security risks. Its use is governed by the Artificial Intelligence Usage Policy.

Staff must only use college-approved AI services for work purposes and in accordance with the Artificial Intelligence Usage Policy. Activate Learning will assess and approve AI systems based on appropriate safety, security and data protection measures and will monitor their use within the organisation.

AI-generated or manipulated content, including synthetic media, deepfakes and voice cloning, can be used to deceive, harass, exploit or impersonate others. Users must not use AI to create, manipulate or distribute unlawful, misleading, harmful, discriminatory, abusive or exploitative content, or content intended to harass or impersonate another person.

Concerns or incidents will be managed under the appropriate organisational policies and may be referred to external agencies, including Social Care, the Local Authority

Designated Officer or Police, where there is a risk of harm or potential criminal offence.

7.3 Social Media and Public Communications

Social media can support communication, collaboration and engagement but also presents safeguarding, professional and reputational risks. Activate Learning promotes safe and responsible use and provides students and apprentices with education on online risks, reporting concerns and accessing support.

Staff must comply with the Social Media Procedure and Professional Conduct Policy. Communication with students and apprentices must take place through approved organisational systems and platforms. Staff and students/apprentices must not connect through personal social media accounts, including professional networking platforms such as LinkedIn. Students and apprentices are discouraged from following staff, governors, volunteers or contractors on public accounts, and staff must not follow public student or apprentice accounts.

Official organisational social media accounts must be appropriately authorised, managed and moderated by the Marketing and Communications Team.

Social media activity presenting a safeguarding, disciplinary, reputational or other organisational concern will be managed through the appropriate procedures.

7.4 Digital Content

Activate Learning recognises the value of photographs, video and other digital content while protecting individuals' privacy, dignity and safety.

Images, recordings and digital content must be collected, stored, used and shared lawfully and in accordance with the UK GDPR, Data Protection Act 2018 and relevant organisational policies.

Staff, students, apprentices, and volunteers must:

- obtain appropriate consent where required;
- use organisation-approved devices to capture images of students during educational activities;
- respect the privacy and dignity of others; and

- not take, share or publish images or recordings without appropriate permission.

Parents and carers may photograph or record their own children at public college events for personal use unless otherwise advised. Content containing other individuals must not be shared publicly without appropriate consent.

Activate Learning may take photographs and recordings at events for promotional and educational purposes, including use on its website, social media, publications and other official communications. Individuals wishing to opt out or withdraw consent should contact the Marketing Team at marketing@activatelearning.ac.uk.

Covert recording, or sharing images intended to harass, intimidate or exploit others, will be treated as a safeguarding concern and managed under the appropriate organisational policies and, where necessary, referred to external agencies.

7.5 Emerging Technologies

Activate Learning recognises that emerging technologies can provide opportunities for learning, communication and accessibility while creating new safeguarding, privacy, security and ethical risks.

This includes wearable technologies such as smart glasses, smart watches and body-mounted cameras. Users must not use such technologies to record, livestream or otherwise capture images, audio or video of staff, students or visitors without appropriate authorisation. Covert recording is prohibited and may constitute a safeguarding concern, disciplinary matter or criminal offence.

The misuse of emerging technologies to harass, intimidate, impersonate, exploit, deceive or facilitate abuse, including through AI-generated or manipulated content, will be managed under the appropriate organisational policies and may be referred to external agencies where necessary.

Activate Learning will continue to review emerging technologies and update guidance and technical controls to ensure they are introduced and used safely, ethically and in accordance with legal and regulatory requirements.

8. Education

8.1 Staff Training

Activate Learning recognises that effective online safety depends on knowledgeable and confident staff.

All staff receive safeguarding, Prevent and online safety training during induction, with regular updates in accordance with statutory guidance and organisational requirements. Training enables staff to understand online safety as part of safeguarding, recognise risks associated with digital and emerging technologies, including AI, and know how to identify, respond to and report concerns.

Digital Education Services further supports staff through professional development aligned to Activate Learning's Digital Competency Framework, promoting the safe, effective and responsible use of digital technologies and AI.

8.2 Online Safety Education

Online safety is embedded within the curriculum and wider student experience through planned, age-appropriate and inclusive education that reflects current risks, emerging technologies and students and apprentices lived experiences.

Our approach is informed by recognised frameworks, including the UK Council for Internet Safety (UKCIS) *Education for a Connected World* Framework, and reinforced through tutorials, enrichment, awareness campaigns and initiatives such as Safer Internet Day.

Students and apprentices are supported to:

- recognise and respond to online risks, abuse and exploitation;
- use technology safely, responsibly and respectfully;
- critically evaluate online information, AI-generated content and misinformation;
- understand privacy, consent, healthy relationships, digital footprints and online reputation;
- recognise harmful online behaviours, including child-on-child abuse, coercion, harmful gender attitudes, and exploitation; and
- know how and where to seek help or report concerns.

The 4Cs framework (Content, Contact, Conduct and Commerce) informs curriculum planning and wider safeguarding education. Online safety resources and reporting information are also available through Activate Learning's digital learning platforms.

8.3 Remote and Blended Learning

Where learning is delivered remotely or through blended approaches, Activate Learning will maintain appropriate safeguarding arrangements in accordance with organisational policies and recognised good practice, including Department for Education guidance on safeguarding and remote education.

The same expectations regarding behaviour, safeguarding, professional conduct and acceptable use apply whether learning takes place on-site or remotely.

Recording, capturing or sharing online learning sessions is only permitted where authorised and in accordance with organisational policies, data protection and privacy requirements. Unauthorised recording, screenshots or redistribution of learning content or communications is prohibited and may result in disciplinary action.

8.4 Student Voice

Activate Learning recognises students and apprentices as key partners in promoting online safety. Learner feedback and experiences are used to identify emerging risks and inform the development of policies, education, campaigns and support services.

Students and apprentices are encouraged to contribute to online safety initiatives and help promote a safe, respectful and positive digital culture across Activate Learning.

9. Safeguarding

9.1 Reporting and Responding to Online Safety Concerns

Despite appropriate education, safeguarding measures and technical controls, online safety incidents may occur within or beyond Activate Learning's learning environments. These may include online abuse, exploitation, Cyberbullying, harassment, discrimination, child-on-child abuse, consensual or non-consensual

sharing of intimate images, sextortion, grooming, fraud, cybercrime, violent or extremist content, harmful sexual behaviour and other illegal or inappropriate activity.

Activate Learning promotes a culture in which concerns are recognised, reported and taken seriously. Students, apprentices, staff, volunteers and visitors should report concerns through the Safeguarding – Reporting a Concern Procedure, including anonymous reporting routes where appropriate. Where there is reason to believe that a child, young person or adult at risk is suffering, or is likely to suffer, significant harm, safeguarding procedures will be followed immediately.

All concerns will be assessed individually, taking account of the nature and severity of the incident, the level of risk, the needs of those involved and any wider safeguarding considerations. Responses will be prompt, proportionate and focused on the welfare of those affected, and may include:

- safeguarding intervention, support and safety planning;
- educational, restorative or behavioural approaches;
- disciplinary action where appropriate;
- technical measures, including changes to filtering, monitoring or system access;
- risk assessment and ongoing monitoring; and
- referral to external agencies, including Children's Social Care, Adult Social Care, Police, the Local Authority Designated Officer (LADO), Prevent partners or specialist services.

Concerns involving staff will be managed under the Professional Conduct Policy, Managing Allegations Against Staff Procedure and relevant HR procedures.

Concerns involving students or apprentices will be managed under the Safeguarding and Prevent Policy, Safeguarding – Reporting a Concern Procedure, Child-on-Child Abuse, Student Harassment and Sexual Misconduct Procedure and Student Positive Behaviour Management Policy.

9.2 Safeguarding Different Groups

Students aged 14–16 – Students in this age group may be particularly vulnerable to online harms. Their age, increasing independence and use of social media and other online platforms may increase exposure to these risks, while their developing understanding of online safety and consequences may affect their ability to recognise and respond to them. Therefore, students aged 14–16 may require additional age-appropriate safeguarding education, support and supervision due to their developmental stage and increasing online independence.

Adult students and apprentices - Adults are generally expected to exercise greater autonomy and responsibility for their online activity. Activate Learning will provide appropriate safeguarding information, education and support to promote digital resilience, informed decision-making, privacy, security and awareness of online risks. However, adulthood does not remove the need for safeguarding. Some adults may be particularly vulnerable due to their individual circumstances or other factors affecting their ability to recognise or respond to online harm.

Students in Higher Education - Higher Education students may encounter challenging, controversial or distressing content through legitimate academic study, research and debate. Safeguarding considerations may include exposure to extremist or harmful material, online harassment, hate or discriminatory content, and harmful or abusive online behaviour. Legitimate academic engagement should be distinguished from activity that presents a safeguarding, criminal or security risk.

Students and apprentices studying predominantly or wholly online - Predominantly or wholly online learners may have greater exposure to online risks due to the frequency and intensity of their digital engagement and reduced visibility where there is limited face-to-face contact. Activate Learning will therefore ensure that online students and apprentices have clear and accessible safeguarding information and reporting routes, appropriate opportunities for welfare contact and access to support.

Residential students – Students living in residential accommodation may face increased safeguarding risks due to living away from home, greater independence and reduced parental supervision. Online risks may be heightened where students use devices privately in bedrooms or other areas without direct staff oversight, increasing potential exposure to online risks. Activate Learning will provide

appropriate residential supervision, safeguarding information, clear reporting routes and access to support.

9.3 Recording and Information Sharing

Online safety concerns meeting safeguarding thresholds will be recorded on CPOMS in accordance with safeguarding recording requirements. Records will be accurate, timely and proportionate to support effective risk assessment, decision-making, action planning and oversight.

Information will be shared on a need-to-know basis and in accordance with the UK GDPR, Data Protection Act 2018 and statutory safeguarding guidance.

9.4 Data Protection and Privacy

Activate Learning processes personal information lawfully, fairly and transparently in accordance with the UK GDPR and Data Protection Act 2018.

Monitoring of activity on organisational systems supports safeguarding, cyber security and legal responsibilities. Access to monitoring information, alerts and logs is restricted to authorised personnel with legitimate safeguarding, information security, HR or technical responsibilities.

Users are informed through the IT Services Acceptable Use Policy that activity on organisational systems and networks may be monitored for safeguarding, security and compliance purposes.

9.5 Prevent and Online Radicalisation

Activate Learning recognises that online environments can expose individuals to extremist and terrorist content and that online radicalisation is a safeguarding concern.

In fulfilling its duties under the Counter Terrorism and Security Act 2015 and the Prevent Duty, Activate Learning will:

- provide online safety and Prevent-related education and awareness;
- maintain appropriate filtering and monitoring arrangements, including recognised terrorism block lists;

- identify and respond to concerns involving extremist or radicalising online content;
- make referrals through Prevent, Channel and safeguarding procedures where appropriate; and
- assess and manage online and other Prevent risks through the Prevent Risk Assessment and Action Plan.

10. Quality Assurance and Continuous Improvement

Activate Learning is committed to maintaining effective online safety arrangements through robust governance, quality assurance and continuous improvement.

This policy is developed and reviewed through consultation with the Safeguarding Committee, Online Safety Working Group and representatives from across the Activate Learning community. It will be reviewed at least annually, or sooner where required in response to changes in legislation, statutory guidance, technology, emerging risks, organisational learning or significant safeguarding incidents.

Strategic oversight is provided by the Safeguarding Committee, which includes Governor representation, members of the Group Executive Team and senior leaders. The Committee receives regular assurance on the effectiveness of the organisation's online safety arrangements.

Activate Learning uses recognised sector tools, including the SWGfL 360 Safe self-review tool and UK Safer Internet Centre Testing Filtering tool, alongside internal quality assurance activity, to assess the maturity and effectiveness of its online safety arrangements and identify areas for improvement.

Findings inform action planning, staff development, technical improvements, learner education and policy development. Progress is monitored through the Online Safety Working Group and reported through governance arrangements to ensure that identified improvements are implemented, and online safety arrangements remain effective and responsive to emerging risks.

11. References

Data Protection Act 2018

Department for Education – Filtering and Monitoring Standards for Schools and Colleges

Department for Education – Keeping Children Safe in Education

Department for Education – Meeting Digital and Technology Standards in Schools and Colleges

Department for Education – Safeguarding and Remote Education

Department for Education – Searching, Screening and Confiscation Advice for Schools

Department for Education – Teaching Online Safety in Schools

Prevent Duty Guidance 2015, Revised 2023

The Education and Inspections Act 2006

South West Grid for Learning – Safer Remote Learning

UKCIS – Education for a Connected World Framework

UKCIS – Sharing Nudes and Semi-Nudes: Advice for Education Settings

UK General Data Protection Regulation

Allegations Against Staff Procedure

Artificial Intelligence (AI) Usage Policy

Child-On-Child Abuse, Student Harassment and Sexual Misconduct Procedure

Compliments, Comments, And Complaints Procedure

Data Protection Procedure

IT Services Acceptable Use Policy and Procedure

Professional Conduct Policy

Safeguarding – Reporting a Concern Procedure

Safeguarding and Prevent Policy

Social Media Procedure

Staff Disciplinary Procedure

Student Positive Behaviour Management Policy

Student Positive Behaviour Management Procedure

Student Search Policy

Student Search Procedure

Appendix 1:

Online Safety Issues

Safeguarding our students and apprentices is of the utmost importance. Staff should be aware of the following key online safety risks:

AI-Generated Abuse – Harmful, deceptive or exploitative content created or manipulated using AI, including sexualised images, deepfakes, voice cloning and impersonation. Creating, possessing or distributing AI-generated child sexual abuse material is illegal in the UK.

Chatbots – AI applications that simulate human conversation. Unsupervised use may expose children or adults at risk to inappropriate content, data collection or harmful influence.

Coerced Online Sexual Abuse – The grooming, coercion or exploitation of children to create sexual images or videos of themselves, including where content is subsequently shared without their knowledge or consent.

Cyberbullying – Bullying, harassment or intimidation carried out through digital technologies or online platforms.

Cyberflashing – Sending unsolicited sexual images or pornography to another person through digital technology.

Deepfakes – AI or computer-manipulated images, video, audio or other media that realistically imitate or alter a person's appearance or voice, with or without their consent.

Disinformation – False or manipulated information deliberately shared to deceive, influence, cause harm or manipulate behaviour, including through extremist narratives, scams and conspiracy theories.

Doxxing – Sharing someone's personal or private information online without consent, potentially exposing them to harassment, stalking, intimidation or harm.

Extremism and Radicalisation – Extremism involves the vocal or active opposition to fundamental British values. Radicalisation is the process through which an individual adopts increasingly extremist views or beliefs. Online spaces may be used to spread extremist content, propaganda and disinformation or to target vulnerable individuals.

Gaming and Livestreaming – Online gaming and real-time broadcasting can expose users to inappropriate content, harmful interactions, exploitation, grooming and other online risks.

Identity Theft – The theft or misuse of personal information, often through techniques such as phishing, social engineering or other online scams.

Incel Ideology and Online Misogyny – Online misogyny includes harmful attitudes, abuse, discrimination or harassment towards women and girls. Some online communities promote incel ideology, which can include misogyny, entitlement, hatred towards women and support for violence.

Misinformation – False or inaccurate information shared without necessarily intending to deceive. Students should be encouraged to critically assess and fact-check online information.

Online Addiction and Compulsive Behaviour – Excessive or compulsive use of gaming, gambling, social media, mobile phones or the internet that may negatively affect wellbeing, learning, relationships or daily life.

Online Challenges and Hoaxes – Online trends or challenges that may encourage harmful, dangerous or illegal behaviour, including harm to individuals or property.

Online Sexual Harassment – Unwanted sexual behaviour in digital spaces, including sexual messages, images, comments, altered photographs or demands for sexual content.

Pornography – Sexually explicit online content which may influence attitudes towards sex, relationships, consent and body image, particularly among children and young people.

Self-Harm and Suicide Content – Online content that promotes, encourages, instructs, glamorises or depicts self-harm, eating disorders or suicide-related behaviour and may increase risks for vulnerable individuals.

Sexting – Sending or receiving sexual messages, images or videos through digital technologies. Where this involves anyone under 18, safeguarding procedures must be followed in accordance with relevant legislation and organisational procedures.

Sextortion – Blackmail involving threats to share sexual images or videos unless the victim pays money or provides further sexual content or acts. Perpetrators may use social media, dating platforms, gaming or other online services and may use false identities.

Sharing Nude or Semi-Nude Imagery – The creation, sending or sharing of nude or semi-nude images, videos or livestreams involving anyone under 18. Creating, possessing or sharing sexual images of a person under 18 is illegal, including where the image was initially created or shared voluntarily.

Trolling – Deliberately provocative, offensive, abusive or disruptive online behaviour intended to upset, anger, intimidate or provoke others.

Appendix 2:

Further Support

The following services provide advice, support and reporting routes for online safety concerns. Staff should follow Activate Learning's safeguarding procedures in the first instance where a student, apprentice or member of staff may be at risk.

- **Activate Learning Safeguarding Team -** Email: safe@activatelearning.ac.uk, Telephone: 01865 550401, Complete the Record of Concern form – internal staff use only
- **Advice and support for professionals dealing with online safety issues -** Email: helpline@saferinternet.org.uk, Telephone: 0344 3814772, Visit the Online Safety Helpline
- **Report terrorism or terrorist content**
- **Act Early –** Prevent support and advice
- **Report Harmful Content**
- **CEOP –** Report online sexual abuse or grooming
- **Internet Watch Foundation –** Report and remove child sexual abuse material
- **Revenge Porn Helpline**

- **StopNCII –** Stop the sharing of intimate images, including deepfakes and AI-generated content
- **Take It Down –** Help to remove or prevent the sharing of nude or sexually explicit images