TITLE	REF	VERSION
Online Safety Policy	LS030	1.0

APPROVAL BODY:	DATE	REVIEW DATE
GET	12 September 2024	12 September 2025

LEAD PERSON	Director - Designated Safeguarding Lead		
EQIA DATE	31 August 2024	DPIA DATE	31 August 2024

ONLINE SAFETY POLICY

Contents

1. Policy Statement

Our vision is to cultivate a safe, supportive, and inclusive learning environment where every learner feels valued, respected, and empowered on their educational journey. In line with our strategic drivers of wellbeing and technology, we want everyone to feel safe in our learning environments (including online) and aim to extend and enliven students' learning, remove barriers by investing in learning technologies, and help staff, students and our communities to navigate changes to the technological context.

The Online Safety Policy outlines Activate Learning's commitment to safeguard members of our community online in accordance with statutory guidance and best practice outlined in documents such as Keeping Children Safe in Education; Working Together to Safeguarding Children; Prevent Duty Guidance; Providing Remote Education; and Meeting Digital and Technology Standards in Schools and Colleges.

2. Commitment Statement

At Activate Learning we want all learners to feel safe, supported and cared for in line with the core values of our Learning Philosophy and Trauma Informed Practice. Through the implementation of this policy, we strive to create a safeguarding culture which prevents and reduces harm online to children and adults at risk and promotes the wellbeing of all learners enrolled across the group including online learners and apprentices, as well as all employees, volunteers, visitors, and contractors.

3. Purpose

The Online Safety Policy:

- Allocates responsibilities for the delivery of the policy and is regularly reviewed in a collaborative manner, taking account of online safety incidents, changes or trends in technology and related behaviours.
- Sets expectations for the safe and responsible use of digital technologies for learning, administration, and communication.
- Describes how Activate Learning will teach learners about how to be safe and responsible online and in how staff should use digital technologies responsibly, protecting themselves and the college and how they should use this understanding to help safeguard learners in the digital world.
- Sets out our safeguarding commitments to responding to online abuse and harmful content.

The Online Safety Policy is designed to supplement various established policies which should be read in conjunction. Such as Activate Learning's IT Services Acceptable Use Policy and Procedure, Safeguarding and Child Protection Policy, Safeguarding – Reporting a Concern Procedure, Professional Conduct Policy, Social Media Policy and Artificial Intelligence Usage Policy.

4. Scope

This policy applies to all members of the Activate Learning community (including staff, learners, volunteers, contractors, partners, parents / carers, visitors, and community users) who have access to and are users of Activate Learning's IT services and digital systems, both in and out of our learning environments. It also applies to the use of personal digital technology on site (where permitted).

5. Responsibilities

To ensure the safeguarding of our community it is vital that all members work together in this collective effort. However, there are some roles which merit additional responsibilities, as described below.

Corporation Board

A member of the Governing Body is appointed the role of safeguarding link Governor (including online safety). They receive regular updates on online safety incidents and the effectiveness of the online safety provision through the Group's Designated Safeguarding Lead and membership of the Safeguarding Committee which the Online Safety working group report to.

Group Executive Team Lead

The Deputy Chief Executive Officer has oversight for safeguarding (including online safety) and chairs the Safeguarding Committee, whereby Activate Learning's online safety provision is reported on. Safeguarding (including online safety) is a regular standing agenda item at Group Executive Team meetings.

The Group Executive Team are responsible for the approval of the Online Safety Policy and for reviewing its effectiveness through an annual report following an audit of our online safety provision utilising the South-West Grid for Learning (SWGfL) 360-degree self-review tool.

Online Safety Lead (Director - Designated Safeguarding Lead)

The Director - Designated Safeguarding Lead (DSL) will work collaboratively with the Group Director of Institutional Effectiveness to perform the functions of the Online Safety Lead role.

The DSL will:

Take lead responsibility for online safety within their safeguarding role, ensuring they receive relevant and regularly updated training to enable them to understand the risks associated with online safety, aware of the potential for serious child protection concerns and have the relevant knowledge to keep children safe while they are online.

The DSL will meet regularly with the safeguarding link Governor and Group Director of Institutional Effectiveness to discuss current issues, review incidents and filtering and monitoring logs, and ensure that annual filtering and monitoring checks are conducted. They will report regularly to the Governing Body, Group Executive Team, and Group Leadership Team regarding the organisation's response to safeguarding and online safety.

The DSL will work collaboratively to promote an awareness of online safety education, raising awareness across the organisation in staff training, curriculum design and engagement with national initiatives. The DSL will ensure staff are aware of the procedures that need to be followed in the event of an online safety incident and adherence with the Safeguarding – Reporting a Concern Procedure.

The DSL will consult with the Group Director of Institutional Effectiveness and technical staff regarding matters relating to digital safety, cybersecurity and systems for filtering and monitoring. This will include reviewing Activate Learning's Online Safety Policy and processes and reviewing logs of incidents to inform online safety developments.

Designated Safeguarding Leads

The DSL, Deputies and Safeguarding Teams are trained in online safety issues and aware of the potential for serious safeguarding issues to arise online.

The Deputies and Safeguarding Teams take day-to-day responsibility for the management of online safety incidents which identify a child protection or safeguarding concern, in line with Activate Learning's Safeguarding and Child Protection Policy, Safeguarding – Reporting a Concern Procedure, and Child-on-Child Abuse Procedure.

Group Director for Faculty and College

Group Directors for Faculty and College, and Group Directors of Group Services will develop a planned and coordinated online safety education programme provided through cross-curricular programmes, tutorials, enrichment events, national initiatives, and opportunities, such as Safer Internet Day.

Teaching and Support Staff

All staff are responsible for ensuring that they have an awareness of current online safety matters, trends and remain up to date with their online safety mandatory training. They

understand that online safety is a core part of safeguarding, and they have read and understood the IT Acceptable Use and Online Safety Policy.

All staff ensure that digital communications with learners and parents/carers should be on a professional level and only carried out using Activate Learning systems. Staff should not use personal platforms, systems, or technologies to communicate with learners e.g., personal social media or email accounts. All staff should model safe, responsible, and professional online behaviour in their own use of technology.

All staff engaged with learners should ensure that learners understand and follow the IT Acceptable Use Policy and comply with the Student Code of Conduct and Student Positive Behaviour Management Policy and should have a zero-tolerance approach to incidents of online-bullying, sexual harassment, discrimination, extremism etc.

In sessions where internet use is pre-planned, learners should be guided by staff to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches. Any inappropriate or harmful content should be reported to Activate Learning's IT Service Desk to ensure that it can be blocked by filtering systems.

As per our Safeguarding Policy and Safeguarding – Reporting a Concern Procedure, all staff should act immediately to prevent harm to learners online or inform the Safeguarding Team if they believe a learner is at risk of harm – online or offline.

In sessions which take place using live-streaming or videoconferencing, staff must have full regard to guidance regarding safe use of remote learning resources.

Network and Technical Staff

It is the organisations responsibility to ensure any outside technology service provider used by Activate Learning carries out all online safety measures that are required.

Network and technical staff are responsible for ensuring that:

- They are aware of and follow the Online Safety Policy.
- The organisations technical infrastructure is secure and is not open to misuse or malicious attack.
- Activate Learning meets the required online safety technical requirements as identified.
- There is clear, safe, and managed control of user access to networks and devices.
- They keep up to date with online safety technical information to effectively carry out their online safety role and inform and update others as relevant.
- The use of technology is regularly and effectively monitored in order that any misuse/attempted misuse can be reported for investigation and action.
- The filtering policy is applied and updated on a regular basis and its implementation is not the sole responsibility of any single person.
- Monitoring software/systems are implemented and regularly updated as agreed in Activate Learning's policies.

IT Provider

Day to day management of filtering and monitoring systems requires the specialist knowledge of both safeguarding and IT staff to be effective. Our IT service provider have technical responsibility for: maintaining filtering and monitoring systems, providing filtering and monitoring reports and completing actions following concerns or checks to systems.

The IT Provider is responsible for ensuring Activate Learning's technical infrastructure is secure and not open to misuse or malicious attack and ensure any misuse is identified and reported to the Group Director of Institutional Effectiveness for investigation and action.

Learners

Learners are responsible for using the Activate Learning's digital technology systems in accordance with the IT Acceptable Use Policy and Procedure, and Online Safety Policy, including personal devices whilst on site (including residential accommodation) and on our networks.

Learners should understand the importance of reporting abuse, misuse or access to inappropriate or harmful materials and know how to do so and should know what to do if they or someone they know feels vulnerable when using online technology.

Learners should understand the importance of adopting good online safety practice when using digital technologies outside of Activate Learning and realise that the Online Safety Policy covers their actions out of our learning and work environments, if related to their membership of Activate Learning.

Guardians

Parents and carers play a crucial role in ensuring that their children understand the need to use the online services and devices in an appropriate way.

Activate Learning will take opportunity to help parents and carers understand these issues through publishing the Online Safety Policy on the organisations website and providing information about online safety campaigns, resources, and literature.

Parents and carers will be encouraged to support Activate Learning in reinforcing the online safety messages provided to learners and in the safe use of their children's IT use when in our learning environments (including their own personal devices).

Community Users

Any users who access Activate Learning's systems and platforms as part of our wider provisions or as a visitor, will be expected to agree to an acceptable use agreement before being provided access and demonstrate these appropriate standards of use.

Activate Learning encourages the engagement of members of our communities and actively seeks to share its knowledge and good practice with other education providers and the wider community.

6. Systems for Online Safety

Online Safety Group

The online safety working group is a consultative group with wide representation from Activate Learning's community, reviewing our online safety provision and impact of initiatives. Members of the group will assist the Online Safety Lead with:

- The review and monitoring of the Online Safety Policy

- Filtering and monitoring provision

- Mapping and review of the online safety education provision for staff, learners, and the wider community

- Consulting with key stakeholders about the online safety provision

- Monitoring improvement actions identified through use of the SWGfL 360-degree self-review tool.

Acceptable Use

The Online Safety Policy and IT Services Acceptable Use Policy define acceptable use within Activate Learning. Acceptable use is communicated and re-enforced through the student Code of Conduct, digital signage, posters, and collateral where technology is used, communication with parents/carers, and built-in to the curriculum.

Filtering

Activate Learning uses filtering services which meets the standards defined by the UK Safer Internet Centre utilising the Internet Watch Foundation CAIC list and Police assessed list of unlawful terrorist content produced by the Home Office. Content is managed across its systems for all users and filter logs are reviewed annually and updated in response to changes in technology and patterns of online safety incidents or behaviours.

The filtering system is applied to all users, including guest accounts, organisation owned devices, and devices using the organisation's broadband connection. Activate Learning have differentiated user-level filtering and enhanced filtering for some groups of learners.

Requests for filtering changes can be made via IT Service Desk to ensure it does not unreasonably impact teaching and learning.

Activate Learning work collaboratively with Oxford Brookes University to ensure appropriate measures are in place at our leased residential accommodation (Harcourt Hill).

Monitoring

Activate Learning has monitoring systems and practices in place to protect the college, systems, and users.

Activate Learning's monitoring system (Smoothwall) sends concerns regarding students to the DSL and Deputies on an instant, daily and weekly basis, alerting them to inappropriate use or harmful content. There are effective protocols in place to report misuse and a clear process for prioritising response to alerts that require rapid safeguarding intervention. Management of serious safeguarding alerts is consistent with Activate Learning's Safeguarding, Child Protection Policy, and Safeguarding – Reporting A Concern Procedure

Alerts relating to staff members are sent to HR for review and triage, and appropriate steps taken to investigate the concern with the staff member's line manager and HR Business

Partner. Weekly reports are also reviewed for searches involving concerns like radicalisation, adult material, or bullying. These are initially examined with further investigation into any areas of significant concern. Minor lapses will result in reminders of the IT Acceptable Use Policy, but serious violations will result in the Staff Disciplinary Procedure being initiated.

All staff should report concerns to IT if: they witness or suspect unsuitable material has been accessed on College systems, they can access unsuitable material, there is failure in the software, there are perceived unreasonable restrictions that affect teaching and learning, or they notice abbreviations or misspellings that allow access to restricted materials.

Staff should report in advance to IT and Safeguarding Teams if they or their students intend to research sensitive topics, as part of legitimate teaching and learning, that may flag as a concern. For example, researching the impact of illicit substances as part of a Health and Social Care or Nursing course.

Vulnerable Learners

Activate Learning recognises that any learner can be vulnerable online, and this can fluctuate. However, there are some learners for example, those with special educational needs, children who are cared for or those in minority groups, who may be more susceptible to online harm such as bullying, discrimination and exploitation. There are also often additional barriers to recognising abuse and neglect in these groups.

Activate Learning tailor our offer to ensure these learners receive the information and support they need. Our filtering and monitoring provisions are also differentiated to meet the needs of specified groups of learners.

Review

To understand and evaluate the changing needs and potential risks of Activate Learning, the filtering and monitoring provision is reviewed at least annually. The review is conducted by the Group Director for Student Experience and Safeguarding, Designated Safeguarding Lead, Group Director for Institutional Effectiveness, and Group IT Systems and Infrastructure Manager. Activate Learning utilise the South-West Grid for Learning 360-degree review tool to audit our provision and progress.

7. Responding to Incidents of Concern (see Appendix 1)

Reporting

Activate Learning will take all reasonable precautions to ensure online safety for all users but recognises that incidents may occur inside and outside of its learning environments that may require intervention.

Activate Learning ensure there are clear reporting routes for reporting online safety incidents, which are understood and followed by all members of our community which are consistent with the Safeguarding and Child Protection Policy, Safeguarding – Reporting a Concern Procedure, Child-on-Child Abuse Procedure, Whistleblowing Policy, Compliments, Comments and Complaints Policy, and Managing Allegations Against Staff Procedure.

Reports will be dealt with in a timely manner, and by Safeguarding staff who have the appropriate skills and training to deal with online safety risks. Where there is any reason to

believe an incident place a student or any other child/young person at significant risk of harm, this will be dealt with in accordance with our Safeguarding Policy.

Any concern regarding staff misuse should be reported to the relevant HR Business Partner in line with the Professional Conduct Policy and Allegations Against Staff Procedures.

Responding

Activate Learning will deal with incidents that involve inappropriate use of IT services, systems, technologies, or devices in a proportionate and fair manner.

Incidents of inappropriate use by staff members will be dealt with by HR in accordance with the Professional Conduct Policy and Staff Disciplinary Procedure. Where the alleged incident indicates a risk of harm to the others, it will be dealt with in conjunction with the Safeguarding Team under the Allegations Against Staff Procedure.

Incidents of inappropriate use of IT by students will be dealt with by the faculty or programme area in line with the Student Positive Behaviour Management Policy and Procedure. Any incidents that indicate a risk of harm to others may also be dealt with in collaboration with the Safeguarding Team in accordance with the Safeguarding and Child Protection Policy, Safeguarding – Reporting a Concern Procedure, and Child-on-Child Abuse Procedure.

As per Activate Learning's IT Services Acceptable Use Policy and Procedure, external agencies, for example the Police or Social Care, may be involved where use of Activate Learning's IT services is considered a criminal offence or indicate a risk of harm to children or adults at risk.

Any misuse of personal mobile technologies or social media that impact on the College, will be dealt with in accordance with the Professional Conduct Policy and Staff Disciplinary Procedure or Student Positive Behaviour Management Policy and Procedure.

Prevent

Under the Counter Terrorism and Security Act 2015, education providers must have due regard to the need to protect people from being drawn into terrorism (the 'Prevent duty'). Activate Learning is committed to fulfilling its Prevent duties and recognises the significant role the internet plays in proliferating terrorist content and the increasing risk of accessing inappropriate and harmful extremist content online.

Activate Learning use filtering as a means of restricting access to harmful content as part of our overall strategy to prevent people from becoming involved in, or supporting, terrorism, and provides education to all regarding the risks of accessing harmful content online.

In addition, Activate Learning perform a yearly Prevent risk assessment which assesses how our learners or staff may be at risk of being radicalised into terrorism, including online. Where specific risks are identified, an action plan is developed outlining the steps taken to mitigate the risk.

8. Multimedia and Advance Technologies

Mobile Technologies and Bring Your Own Devices (BYOD)

Activate Learning recognises the widespread use of mobile technologies amongst adults and children of all ages and understand that by effectively maximising use of a range of web-based tools, resources, and content, we can deepen learning and develop our digital competencies, preparing learners for the high-tech world in which they will live, learn, and work.

Mobile technology devices might include smartphone, tablet, wearable devices, notebook, laptop, or other technology that usually has the capability of utilising Activate Learning's wireless network.

All users should understand that the primary purpose of the use of mobile technologies in Activate Learning's context is educational, irrespective of whether the device is college owned/provided or personally owned. Therefore, use of mobile technologies in college is permitted but should not unduly disrupt or adversely affect the teaching, learning, work and/or experience of themselves or others.

All users should be aware that filtering and monitoring systems remain in place when users connect any mobile devices to the college's networks and attempts to bypass this are not permitted. However, Activate Learning recognises that personal devices are often used by staff and students without accessing our secure networks, essentially providing unmonitored access to the internet. Activate Learning take steps to educate staff and students about the risks posed online and how they can seek support should they have concerns for their own or somebody else's safety or welfare.

As per the Student Search Procedure and Department for Education guidance on 'Searching, Screening and Confiscation at School', Activate Learning can search and confiscate a learner's personal device if a member of staff reasonably suspects that the device has been, or could be used, to cause harm, undermine the safe environment of the college and disrupt teaching, or be used to commit an offence.

As per the IT Acceptable Use Policy and Procedure, Activate Learning may at any time and without prior notice audit any college owned devices or require the return of these devices and any associated equipment.

All users should be aware that personal devices are brought onto Activate Learning premises entirely at the risk of the owner. Activate Learning accepts no responsibility or liability in respect of lost, stolen, or damaged devices while on our premises or on activities organised or undertaken by the organisation.

Generative Artificial Intelligence (AI)

Activate Learning recognises the transformative potential of artificial intelligence (AI) and commits to harnessing it for educational excellence and business efficacy. Activate Learning's Artificial Intelligence Usage Policy sets out its approach to the appropriate use of AI within our learning environments to maximise the benefits of AI while reducing risks and ethical concerns.

Activate Learning recognises that synthetic media (media generated with the help of AI) can offer creative opportunities when used appropriately. However, as it can also pose risks, as it often appears realistic and may be difficult to distinguish from genuine media.

Synthetic harmful content (e.g., voice cloning, ‘deepfakes’) is any type of media created or altered using AI with the intent to deceive, misinform, harm or exploit others and can have significant implications on privacy, security, misinformation and safeguarding.

The use of synthetic harmful content by staff or students will be dealt with in accordance with Activate Learning’s Student Positive Behaviour Management Policy and Staff Professional Conduct Policy and may be reported to external agencies such as Social Care and Police if it is considered a criminal offence or indicate a risk of harm to children or adults at risk.

Social Media

Activate Learning takes reasonable steps to minimise risk of harm to staff and learners via social media platforms. Education is provided to learners regarding social media risks, and routes for reporting concerns on these platforms and to Activate Learning’s student support teams.

Activate Learning staff should adhere to the Social Media Procedure for guidance relating to their own use of social media.

Activate Learning respects privacy and understands that staff and students may use social media forums in their private lives. However, personal communications likely to have a negative impact on professional standards and/or the organisations reputation are within the scope of this policy.

Professional communications are those made through official channels, posted on any Activate Learning endorsed account or using Activate Learning (or associated College’s) name.

Personal communications are those made via a personal social media account. In all cases, where a personal account is used which associates itself with, or impacts on, Activate Learning, it must be made clear that the member of staff is not communicating on behalf of the organisation with an appropriate disclaimer. Such professional and personal communications are within the scope of this policy.

Digital communications between staff and students via personal social media accounts (including professional networking accounts such as LinkedIn) is not permitted. Under no circumstances should staff share or upload learner pictures online other than via official and approved channels.

When official social media accounts are established, there should be a process for approval by senior leaders, clear processes for the administration, moderation, and monitoring of these accounts – involving at least two members of staff, a code of behaviour for users of the accounts and systems for reporting and dealing with abuse and misuse, though ensuring that personal information is not published on Activate Learning’s social media platforms.

As part of active social media engagement, the organisation may pro-actively monitor the Internet for public postings about Activate Learning. The Marketing and Communications Team will effectively respond to social media comments made by others according to a defined policy or process.

When parents/carers or members of the community express concerns about the organisation on social media they will urge them to make direct contact with the college, in

private, to resolve the matter. Where this cannot be resolved, they should be informed of Activate Learning's Compliments, Comments, and Complaints Procedure.

Digital and Video Images

Activate Learning understands that sharing photographs and films of our activities can help us celebrate the successes and achievements of our learners, provide a record of our activities and raise awareness of our organisation. However, the welfare of learners taking part in our activities is paramount and acknowledge there are potential risks associated with sharing images of children online.

We will seek to keep learners safe by: seeking consent before taking and using a learner's image, explaining what images will be used for and how they will be stored, making it clear that they may withdraw consent for an image to be shared, but that it may not be possible to delete images that have already been shared or published, and never publishing personal information about individual children and disguising any identifying information. Activate Learning will also inform and educate staff and learners about risks associated with publishing digital images and videos online.

Staff, students and volunteers may take digital/video images to support educational aims but must seek consent and follow Activate Learning's Data Protection Procedure concerning the sharing, storage, distribution, and publication of those images. Taking of images or recordings of others without their consent is not permitted.

Activate Learning does not permit staff and volunteers to using any personal equipment to take photos and recordings of learners. Only cameras or devices belonging to the organisation should be used.

During Activate Learning events, we may take photographs or recordings. These may be published via multiple channels, including social media, the Activate Learning website and print media. If you do not wish to be included in these group photographs, staff and students can request this via the Marketing Team.

In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at college events for their own personal use. To respect everyone's privacy and in some cases protection, these images should not be published and made publicly available on social networking sites, nor should parents/carers comment on any activities involving other learners in the digital/video images.

9. Teaching and Learning

Training

All staff are required to undergo safeguarding and child protection, and online safety training as part of their induction and regularly updated. Additional safeguarding and child protection updates, including online safety, are provided at least annually, ensuring staff are continually provided with relevant skills and knowledge to safeguard learners effectively.

All staff are aware that technology is a significant component in many safeguarding and wellbeing issues, and students can be at risk online as well as face to face. Staff are aware that children can also abuse other children online.

Activate Learning's Digital Education Services support with the development of digital knowledge, skills and mindset of staff by providing additional resources and training on Activate Learning's 6C's of Digital Competencies (creating, communicating, collaborating, curating, connecting, and critical thinking) and lead the organisation's research and response for Artificial Intelligence.

Opportunities for Teaching and Learning

Learners are taught about how to keep themselves and others safe, including online. Activate Learning utilise the 4Cs (content, contact, conduct and commerce) as a basis for curriculum design, and ensure this is a running and interrelated theme amongst other opportunities for teaching and learning about safeguarding. Teaching is tailored to meet the specific needs of learners.

Remote Learning

Activate Learning may use live-streaming or video conferencing services to provide remote education in line with national and local safeguarding guidance such as SWGfL Safer Remote Learning and DfE Safeguarding and Remote Education.

Learners and staff should be aware that the same principles set out in Activate Learning's policies and procedures apply.

Staff and learners should seek consent before recording online sessions, making sure all parties understand why the recording is necessary, how it will be securely stored and what will happen with the recording.

10. Review

This policy has been developed by members of the Safeguarding Committee and Online Safety working group. Consultation with the wider community has taken place through a range of formal and informal meetings.

It will be reviewed annually by the Safeguarding Committee made up of a Governor, Group Executive, Senior Leadership Team members and Director - Designated Safeguarding Lead.

Activate Learning will monitor the impact of the policy through the Online Safety working group, using a variety of means such as logs of reported incidents, internal monitoring data for network activity, filtering and monitoring logs, and surveys to members of our community. Activate Learning's online safety provision is audited annually utilising the South-West Grid for Learning 360-degree tool.

11. References

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

The Education and Inspections Act 2006

Copies of the below documents can be found on the Policy and Procedure app here.

Allegations Against Staff Procedure

Artificial Intelligence Usage Policy

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 Child Protection Policy

Social Media Procedure

South-West Grid for Learning Safer Remote Learning

Staff Disciplinary Procedure

Student Positive Behaviour Management Policy

Student Positive Behaviour Management Procedure

Student Search Policy

Student Search Procedure

Appendix 1:

Online Issues

Safeguarding our student's is of utmost importance to Activate Learning. Below are some key online safety issues:

Addiction - Addiction is most commonly associated with aspects such as drugs, gambling and alcohol, but it can also describe a broad range of online behaviours, such as online gaming addiction (internet gaming disorder), online gambling addiction, social media addiction, mobile phone addiction, or even just internet addiction in general.

Artificial Intelligence Generated Abuse – Artificial Intelligence (AI) refers to the simulation of human intelligence processes by machines, especially computer systems. AI is being used to generate indecent images of children. Child sexual abuse images are illegal in the UK, regardless of how it is produced.

Chatbots - A chatbot is a software application that is designed to mimic human conversation through text or voice interactions. Children using chatbots face potential risks such as exposure to inappropriate content, privacy breaches through data collection, and vulnerability to cyberbullying or spreading of misinformation.

Coerced Online Sexual Abuse - Children can be groomed, coerced, or encouraged into sexual activities online. This is known as self-generated child sexual abuse content. It's where sexual images or videos of children are captured via a webcam or camera-enabled device. There is no physical presence of the abuser, and the child is often in their own home. Whilst these images can be the product of grooming, blackmail, and coercion, they could have also been originally voluntarily produced by the child, but then shared with others without the child's full knowledge or consent. Any child with unsupervised access to the internet is potentially at risk.

Cyberbullying – Cyberbullying is when someone uses the internet to bully someone else.

Cyberflashing - 'Cyberflashing' is where somebody digitally sends sexual images or pornography to an unsuspecting person. Due to the nature of channels used to send these images, the victim will not know they have been cyberflashed until they have actively opened the notification or gone into the app.

Deepfake - A deepfake is an image, video, sound, voice, or GIF which has been manipulated by a computer to superimpose someone's face, body, or voice onto something else. This could be done with or without the subject's consent.

Extremism - Defined as 'the vocal or active opposition to fundamental British values, including democracy, the rule of law, individual liberty and mutual respect and tolerance of different faiths and beliefs,' extremism refers to an ideology considered to be outside the mainstream attitudes of society. Radicalisation is the process where someone changes their perception and beliefs to become more extremist.

Extremists use the online space to target and exploit vulnerable people, and to spread divisive propaganda and disinformation.

Gaming and Livestreaming – Livestreaming is when an individual or a group of people broadcast themselves or others to an audience online in real-time. Many social media platforms offer a livestreaming feature that is available to anyone but often used by gamers, celebrities, or influencers to communicate with a chosen audience.

Identity Theft - Is when your personal/private details are stolen. Criminals are increasingly using technology in more complex ways, often using social engineering tricks such as fear or urgency to lure people into revealing personal and private information, for example phishing scams.

Misinformation - Misinformation or 'fake news' is online content that can mislead or provide false information towards a particular topic. Stories can often be fabricated to cause panic or concern and heavily rely on users to critically determine what is trustworthy or not.
Staff should educate students on how to 'fact-check' information.

Online Challenges – Online challenges or hoaxes can commonly appear on social media or other platforms. The 'challenges' themselves can vary but often encourage individuals to harm themselves, others, or property in the real world. They are often created to cause alarm and have been designed to seem enticing or exciting for young people.

Online Sexual Harassment – Online Sexual Harassment is unwanted sexual contact on a digital device which negatively impacts another person. This can take many forms (both take place both online and offline) such as unwanted sexualised messages, sharing unsolicited intimate imagery, requesting sexualised messages or imagery, doctoring, or editing imagery to make people appear to be in intimate or sexualised situations, sexualised insults or name-calling, leaving sexually suggestive comments on someone's online content.

Pornography – Online pornography can be images or videos online of naked adults, adults having sexual intercourse, or showing sexual behaviour. Pornography, both online and offline, can influence how they think about sex, relationships and their own body image.

Sexting – Sexting is the communication between individuals that involves sexual content. This can be through text messages, images, or videos. Very often it is between partners but can be between groups or friends. It can spread across a whole range of devices, technologies, and online spaces.

Sextortion – 'Sextortion' mis a form of blackmail. It involves threatening to publish sexual information, photos, or videos about someone. This may be to extort money or to force the victim to do something against their will. Photos or recordings are often made without the victim realising or consenting. Criminals often target people through dating apps, social media, webcams, or pornography sites. They may use a fake identity to befriend you online and then threaten to send images to your family and friends.

Sharing Nude and Semi-Nude Imagery – The sending or posting of nude or semi-nude images, videos, or live streams online by young people under the age of 18. Alternative terms used by children and young people may include 'dick pics' or 'pics'. Adults sharing nudes or semi-nudes of under 18-year-olds is a form of child sexual abuse and is a criminal offence.

Appendix 2:

Further Support:

Activate Learning Safeguarding Team –
Email: safe@activatelearning.ac.uk
Call: 01865 550401
Complete a record of concern - Link to record of concern form

Safer Internet Professionals Online Safety Helpline -
Email: helpline@saferinternet.org.uk
Call: 0344 3814772
https://saferinternet.org.uk/professionals-online-safety-helpline

Report Online Material Promoting Terrorism or Extremism –
https://www.gov.uk/report-terrorism
https://actearly.uk/contact/

Report Harmful Content –
https://reportharmfulcontent.com/

Revenge Porn Helpline –
https://revengepornhelpline.org.uk/

Report Online Child Sexual Abuse Material –
https://www.iwf.org.uk/en/uk-report/