Online Safety Policy

Activ8 Education Group

Author/Owner (Name and Title)	Owen Wedgwood
Version Number	Version 2
Date Approved/Reviewed	March 2024
Date of Next Review	September 2024

Contents Page

1. Scope of the Policy

This policy applies to all members of the Activ8 community (including staff, pupils, volunteers, visitors) who have access to and are users of the ICT systems.

Activ8 will deal with such incidents within this policy and will, where known, inform parents / carers of incidents of inappropriate Online Safety behaviour that take place out of the Academy.

2. Roles and Responsibilities

The following section outlines the online safety roles and responsibilities of individuals and groups within the Trust and its academies:

Senior Leaders

- The MD/CEO has a duty of care for ensuring the safety (including online safety) of members of Activ8.
- The MD/CEO and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious online safety allegation being made against a member of staff. (See flow chart on dealing with online safety incidents – included in a later section – "Responding to incidents of misuse").
- The MD/CEO is responsible for ensuring that the Designated Safeguarding Lead and other relevant staff receive suitable training to enable them to carry out their online safety roles and to train other colleagues, as relevant.

Designated Safeguarding Lead – (Online Safety Lead)

- takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the Activ8's online safety policies/documents
- ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place.
- provides training and advice for staff
- liaises with school partners as deemed appropriate.
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments.
- Should be trained in Online Safety issues and be aware of the potential for serious child protection / safeguarding issues to arise from:
  - sharing of personal data
  - access to illegal/inappropriate materials
  - inappropriate on-line contact with adults/strangers
  - potential or actual incidents of grooming
  - cyber-bullying

Delivery Staff

Are responsible for ensuring that**:**

- they have an up to date awareness of online safety matters
- they report any suspected misuse or problem to the CEO/MD Leader/Safeguarding Lead for investigation/action/sanction
- all digital communications with students/pupils/parents/carers should be on a professional level and only carried out using official Activ8 systems
- Children attending sessions understand and follow the Online Safety Policy and acceptable use policies.
- they monitor the use of digital technologies, mobile devices, cameras etc in sessions (where allowed) and implement current policies with regard to these devices

Pupils

- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Will be expected to know and understand policies on the use of mobile devices and digital cameras. They should also know and understand policies on the take/use of images and online-bulling

3. Policy Statements

Education & Training – Staff / Volunteers

It is essential that all staff receive online safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- A planned programme of formal online safety training will be made available to staff. This will be regularly updated and reinforced. An audit of the online safety training needs of all staff will be carried out regularly.
- All new staff should receive online safety training as part of their induction programme, ensuring that they fully understand Activ8's Online Safety Policy.
- The Designated Safeguarding Lead will receive regular updates through attendance at external training events and by reviewing guidance documents released by relevant organisations.
- The Designated Safeguarding Lead will provide advice/guidance/training to individuals as required.

4. Mobile Technologies

Mobile technology devices may be Activ8 provided or personally owned and might include: smartphone, tablet, notebook/laptop or other technology that usually has the capability of utilising wireless networks.

All users should understand that the primary purpose of the use mobile/personal devices in a work context is educational.

Personal devices:

- Personal mobile devices can be brought into Activ8 delivery sites
- Staff will be allowed to use personal devices for Activ8 business should no other devices be made available to them
- Network/broadband capacity is the responsibility of the user
- Technical support is the responsibility of the user
- Filtering of the internet connection to these devices is the responsibility of the user
- Personal devices should not be used for sensitive Activ8 data which might breach Data Protection regulations
- Activ8 has the right to take, examine and search users devices in the case of misuse
- Taking/storage/use of Activ8 images of pupils or staff without their consent is not permitted
- Liability for loss/damage or malfunction is the user's responsibility
- Data Protection is the responsibility of the user
- Users must be made aware that Activ8 has the right to take, examine and search users' devices in the case of misuse (must be included in the behaviour policy)

5. Use of Digital and Video Images

The development of digital imaging technologies has created significant benefits to learning, allowing staff and instant use of images that they have recorded themselves or downloaded from the internet. However, staff need to be aware of the risks associated with publishing digital images on the internet. Such images may provide avenues for cyberbullying to take place. Digital images may remain available on the internet forever and may cause harm or embarrassment to individuals in the short or longer term. It is common for employers to carry out internet searches for information about potential and existing employees. Activ8 will inform and educate users about these risks:

- When using digital images, staff should be aware and inform and educate pupils of the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.
- Written permission from parents/carers will be obtained before photographs of pupils are published on the academy/trust websites/social media/local press.
- Staff and volunteers are allowed to take digital/video images to support educational aims, but must follow Activ8 policies concerning the sharing, distribution and publication of those images. Those images should only be taken on Activ8 equipment; the personal equipment of staff should not be used for such purposes.

- Care should be taken when taking digital/video images that pupils are appropriately dressed and are not participating in activities that might bring the individuals or Activ8 into disrepute.
- Pupils must not take, use, share, publish or distribute images of others without their permission
- Pupils' full names will not be used anywhere on a website or blog, particularly in association with photographs.
- Pupil's work can only be published with the permission of the pupil and parents or carers.
- In accordance with guidance from the Information Commissioner's Office, parents/carers are welcome to take videos and digital images of their children at Activ8 events for their own personal use (as such use in not covered by the Data Protection Act). To respect everyone's privacy and in some cases protection, these images should not be published/made publicly available on social networking sites, nor should parents/carers comment on any activities involving other *students/pupils* in the digital/video images.
- Photographs published on the website, or elsewhere that include pupils will be selected carefully and will comply with good practice guidance on the use of such images.

6. Data Protection

Personal data will be recorded, processed, transferred and made available according to the current data protection legislation which states that personal data must be:

- Fairly and lawfully processed
- Processed for limited purposes
- Adequate, relevant and not excessive
- Accurate
- Kept no longer than is necessary
- Processed in accordance with the data subject's rights
- Secure
- Only transferred to others with adequate protection.

Activ8 must ensure that:

- It has a Data Protection Policy
- It implements the data protection principles and is able to demonstrate that it does so through use of policies, notices and records.
- it has an 'information asset register' in place and knows exactly what personal data it holds, where this data is held, why and which member of staff has responsibility for managing it

- The information asset register records the lawful basis for processing personal data (including, where relevant, how consent was obtained and refreshed). Where special category data is processed, an additional lawful basis will have also been recorded
- Data Protection Impact Assessments (DPIA) are carried out where necessary. For example, to ensure protection of personal data when accessed using any remote access solutions, or entering into a relationship with a new supplier (this may also require ensuring that data processing clauses are included in the supply contract or as an addendum)
- it has undertaken appropriate due diligence and has required data processing clauses in contracts in place with any data processors where personal data is processed.
- it understands how to share data lawfully and safely with other relevant data controllers.
- it reports any relevant breaches to the Information Commissioner within 72hrs of becoming aware of the breach in accordance with UK data protection law. It also reports relevant breaches to the individuals affected as required by law. In order to do this, it has a procedure for reporting, logging, managing, investigating and learning from information risk incidents.
- It will hold the minimum personal data necessary to enable it to perform its function and it will not hold it for longer than necessary for the purposes it was collected for.
- Every effort will be made to ensure that data held is accurate, up to date and that inaccuracies are corrected without unnecessary delay.
- All personal data will be fairly obtained in accordance with the "Privacy Notice" and lawfully processed in accordance with the "Conditions for Processing".
- It has clear and understood arrangements for the security, storage and transfer of personal data
- Data subjects have rights of access and there are clear procedures for this to be obtained
- There are clear and understood policies and routines for the deletion and disposal of data
- There are clear Data Protection clauses in all contracts where personal data may be passed to third parties.

Staff must ensure that they:

- At all times take care to ensure the safe keeping of personal data, minimising the risk of its loss or misuse.

- Use personal data only on secure password protected computers and other devices, ensuring that they are properly “logged-off” at the end of any session in which they are using personal data.
- Transfer data using encryption and secure password protected devices.
- can recognise a possible breach, understand the need for urgency and know who to report it to within the Academy
- can help data subjects understands their rights and know how to handle a request whether verbal or written. Know who to pass it to in the Academy

When personal data is stored on any portable computer system, memory stick or any other removable media:

- the data must be encrypted and password protected
- the device must be password protected
- the device must offer approved virus and malware checking software
- the data must be securely deleted from the device once it has been transferred or its use is complete

7. Communications

A wide range of rapidly developing communications technologies has the potential to enhance learning. The following table shows how the Activ8 currently considers the benefit of using these technologies for education outweighs their risks / disadvantages:

	Staff & other adults

Communication Technologies	Allowed	Allowed at certain times	Allowed for selected staff
Mobile phones may be brought to delivery site	x		
Use of mobile phones in social time	x		
Taking photos on mobile phones / cameras			X
Use of other mobile devices e.g. tablets	x		
Use of messaging apps	x		
Use of social media			x
Use of blogs			x

When using communication technologies, Activ8 considers the following as good practice:

- The Activ8 email service may be regarded as safe but not secure and can be monitored. Users should be aware that email communications can be monitored.
- Users must immediately report, to the nominated person, the receipt of any communication that makes them feel uncomfortable, is offensive, discriminatory, threatening or bullying in nature and must not respond to any such communication.
- Any digital communication between staff that is Activ8 related i.e. emails must be professional in tone and content. These communications may only take place on official Activ8 systems. Personal email addresses, text messaging or social media must not be used for these communications.
- Personal information should not be posted on any Activ8 material and only official email addresses should be used to identify members of staff.

8. Social Media - Protecting Professional Identity

Activ8 have a duty of care to provide a safe learning environment for pupils and staff. Activ8 could be held responsible, indirectly for acts of its employees in the course of their employment. Staff members who harass, cyberbully, discriminate on the grounds of sex, race or disability or who defame a third party may render Activ8 liable to the injured party. Reasonable steps to prevent predictable harm must be in place.

Activ8 provides the following measures to ensure reasonable steps are in place to minimise risk of harm to pupils, staff and Activ8 through:

- Ensuring that personal information is not published
- Training is provided including: acceptable use; social media risks; checking of settings; data protection; reporting issues.
- Clear reporting guidance, including responsibilities, procedures and sanctions
- Risk assessment, including legal risk
- Insurance protection to cover the costs of restoring and protecting data in the event of a cyber-attack on the network

Activ8 staff should ensure that:

- No reference should be made in social media to pupils, parents/carers or Activ8 staff
- They do not engage in online discussion on personal matters relating to members of the Activ8 community
- Personal opinions should not be attributed to Activ8
- Security settings on personal social media profiles are regularly checked to minimise risk of loss of personal information

Personal Use:

- Personal communications are those made via a personal social media accounts. In all cases, where a personal account is used which associates itself with Activ8 or impacts on the Activ8, it must be made clear that the member of staff is not communicating on behalf of Activ8 with an appropriate disclaimer. Such personal communications are within the scope of this policy
- Personal communications which do not refer to or impact upon Activ8 are outside the scope of this policy
- Where excessive personal use of social media in Activ8 is suspected, and considered to be interfering with relevant duties, disciplinary action may be taken
- Activ8 permits reasonable and appropriate access to private social media sites

Monitoring of Public Social Media:

- As part of active social media engagement, it is considered good practice to pro-actively monitor the Internet for public postings about Activ8
- Activ8 should effectively respond to social media comments made by others

9. Unsuitable / Inappropriate Activities

Some internet activity e.g. accessing child abuse images or distributing racist material is illegal and would obviously be banned Activ8 and all other technical systems. Other activities e.g. cyber-bullying would be banned and could lead to criminal prosecution. There are however a range of activities which may, generally, be legal but would be inappropriate in an Activ8 context, because of the nature of those activities.

Activ8 believes that the activities referred to in the following section would be inappropriate in an Activ8 context and that users, as defined below, should not engage in these activities in/or outside of Activ8 when using Activ8 equipment or systems. The Activ8 policy restricts usage as follows:

User Actions		Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Users shall not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to:	Child sexual abuse images –The making, production or distribution of indecent images of children. Contrary to The Protection of Children Act 1978					X
	Grooming, incitement, arrangement or facilitation of sexual acts against children Contrary to the Sexual Offences Act 2003.					X
	Possession of an extreme pornographic image (grossly offensive, disgusting or otherwise of an obscene character) Contrary to the Criminal Justice and Immigration Act 2008					X
	Criminally racist material in UK – to stir up religious hatred (or hatred on the grounds of sexual orientation) - contrary to the Public Order Act 1986					X
	Pornography				X	
	Promotion of any kind of discrimination				X	
	threatening behaviour, including promotion of physical violence or mental harm				X	
	Promotion of extremism or terrorism				X	
	Any other information which may be offensive to colleagues or breaches the integrity of the ethos of Activ8 or brings Activ8 into disrepute				X	
Activities that might be classed as cyber-crime under the Computer Misuse Act:						x

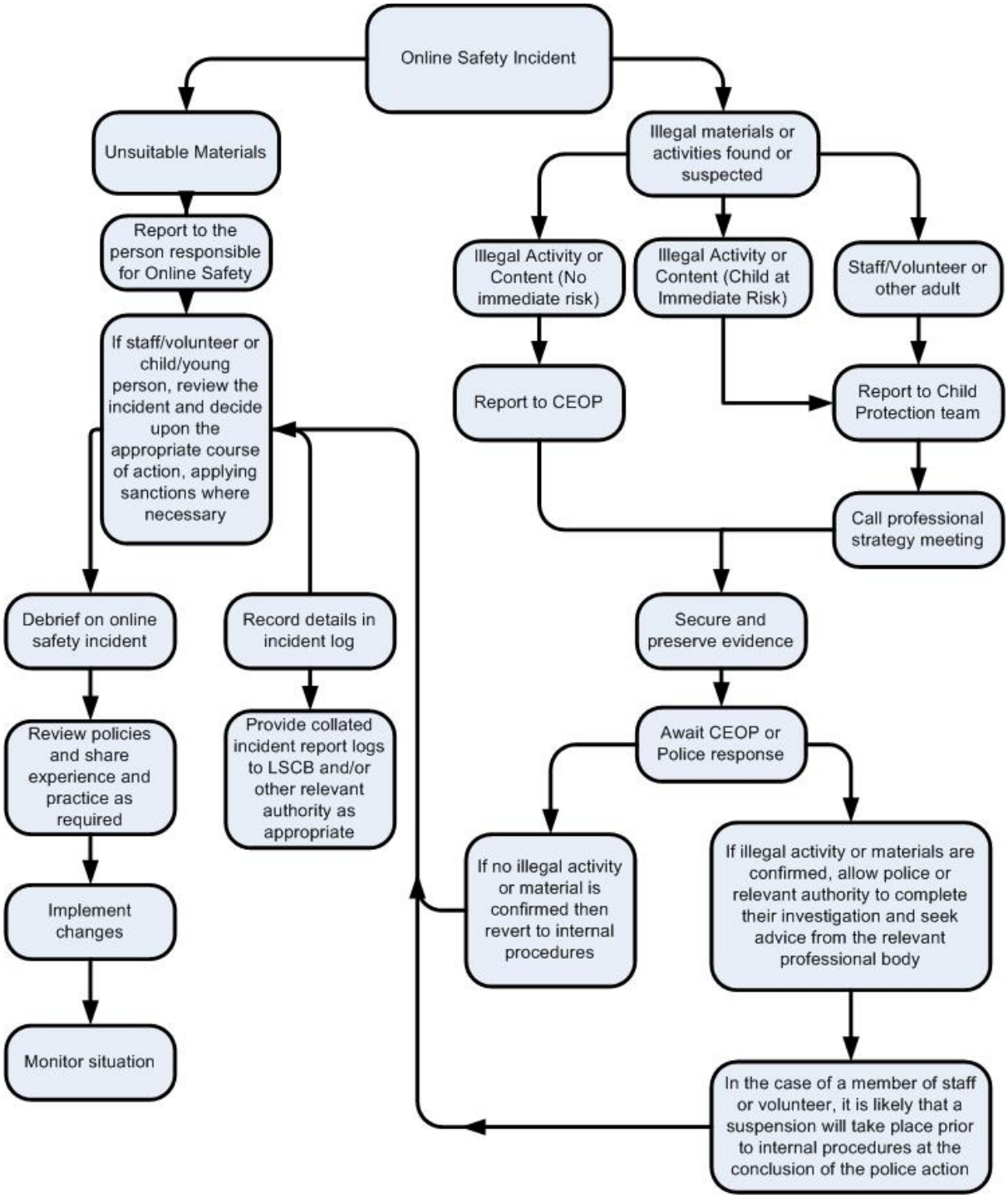
• Creating or propagating computer viruses or other harmful files • Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords) • Disable/Impair/Disrupt network functionality through the use of computers/devices • Using penetration testing equipment (without relevant permission)					
Infringing copyright				X	
Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)				X	
Unfair usage (downloading / uploading large files that hinders others in their use of the internet)				X	
On-line gaming (educational)				x	
On-line gaming (non-educational)				x	
On-line gambling				x	
On-line shopping / commerce		x			
File sharing		x			
Use of social media		x			
Use of messaging apps		x			
Use of video broadcasting e.g. YouTube		x			

10. Responding to Incidents of Misuse

This guidance is intended for use when staff need to manage incidents that involve the use of online services. It encourages a safe and secure approach to the management of the incident. Incidents might involve illegal or inappropriate activities (see "User Actions" above).

11. Illegal Incidents

If there is any suspicion that the web site(s) concerned may contain child abuse images, or if there is any other suspected illegal activity, refer to the right hand side of the Flowchart for responding to online safety incidents and report immediately to the police.



12. Other Incidents

It is hoped that all members of the Activ8 community will be responsible users of digital technologies, who understand and follow the Activ8 policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse.

In the event of suspicion, all steps in this procedure should be followed:

- Have more than one senior member of staff involved in this process. This is vital to protect individuals if accusations are subsequently reported.
- Conduct the procedure using a designated computer that will not be used by young people and if necessary can be taken off site by the police should the need arise. Use the same computer for the duration of the procedure.
- It is important to ensure that the relevant staff should have appropriate internet access to conduct the procedure, but also that the sites and content visited are closely monitored and recorded (to provide further protection).
- Record the URL of any site containing the alleged misuse and describe the nature of the content causing concern. It may also be necessary to record and store screenshots of the content on the machine being used for investigation. These may be printed, signed and attached to the form (except in the case of images of child sexual abuse – see below)
- Once this has been completed and fully investigated it will need to be judged whether this concern has substance or not. If it does then appropriate action will be required and could include the following:
    - Internal response or discipline procedures
    - Police involvement and/or action

If content being reviewed includes images of Child abuse then the monitoring should be halted and referred to the Police immediately. Other instances to report to the Police would include:

- incidents of 'grooming' behaviour
- the sending of obscene materials to a child
- adult material which potentially breaches the Obscene Publications Act
- criminally racist material
- promotion of terrorism or extremism
- other criminal conduct, activity or materials
- offences under the Computer Misuse Act (see Users Actions chart above)

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

It is important that all of the above steps are taken as they will provide an evidence trail for Activ8 and possibly the Police and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained for evidence and reference purposes.