Co-op Academy
Swinton

Online Safeguarding Policy

January 2020

Co-op Academy Swinton, Sefton Road, Pendlebury, Manchester M27 6JU Tel: 0161 794 6215 www.swinton.coop

Introduction

The academy Online Safeguarding Policy applies to all members of the academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of academy ICT systems and mobile technologies, both in and out of the academy.

At Co-op Academy Swinton we understand the responsibility to educate our students in online issues, teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the Internet and related technologies in, and beyond the context of the classroom.

Both this policy and the Acceptable Use Agreement are inclusive of both fixed and mobile internet technologies provided by the school (such as PCs, laptops, personal digital assistants (PDAs), tablet PCs, webcams, whiteboards, voting systems, digital video equipment, digital cameras, visualisers etc.); and technologies owned by students and staff brought onto academy premises such as laptops, mobile phones etc.

Policy Governance:

Development, Monitoring and Review of this Policy

This Online Safeguarding Policy has been developed by a working group/committee comprising:

Position	Name(s)
School Online Safeguarding Officer	Sarah Withers
Deputy Headteacher/ Academy Online Safeguarding Coordinator	Sarah Withers
Teacher	Lindsay Hamer
Senior Human Resources Manager	Carol Robinson
Governor	Malcolm Dodd
Parents	Sue Sparrow

Schedule for Review:

The implementation of this Online Safeguarding Policy will be monitored by:	Sarah Withers, Deputy Headteacher Lindsey Hamer, Online Safeguarding Officer Senior Leadership Team
Monitoring will take place at regular intervals:	Annually
The Governing Body will receive a report on the implementation of the Online Safeguarding Policy generated by the monitoring group at regular intervals:	Annually
The Online Safeguarding Policy will be reviewed annually, or more regularly in the light of any significant new developments in the use of the technologies, new threats to online safety or incidents that have taken place. The next anticipated review date will be:	January 2020
Should serious online incidents take place, the following external persons/agencies should be informed:	Novus Safeguarding Officer (Bridge Team) Police Commissioner's Office

Scope of the Policy

This policy applies to all members of the academy community (including staff, students, volunteers, parents/carers, visitors, community users) who have access to and are users of school ICT systems and mobile technologies, both in and out of the academy.

Roles and Responsibilities

The following section outlines the roles and responsibilities for Online Safeguarding of individuals and groups within the school:

Governors:

- Governors are responsible for the approval of the Online Safeguarding Policy and for reviewing the effectiveness of the policy.
- Governors should have no expectations of privacy of academy email accounts, as the e-mails are meant for business communications

Headteacher and Senior Leaders:

- The Headteacher is responsible for ensuring the safety (including online safeguarding) of members of the academy community
- The Headteacher and another member of the Senior Leadership Team/Senior Management Team should be aware of the procedures to be followed in the event of a serious online safeguarding allegation being made against a member of staff
- The Headteacher and senior leaders should have no expectations of privacy of academy email accounts, as the e-mails are meant for business communications

Online Safeguarding Coordinator/Officer:

Miss Sarah Withers, Deputy Headteacher (Online Safeguarding Co-ordinator) and Miss Lindsey Hamer (Online safeguarding Officer)

- Lead the Online Safeguarding Committee and/or cross-school initiative on Online safety
- Takes day-to-day responsibility for online safeguarding issues and has a leading role in establishing and reviewing the academy online safeguarding policies/documents
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safeguarding incident taking place.
- Provides training and advice for staff
- Receives reports of online safeguarding incidents and creates a log of incidents to inform future online safeguarding developments
- Reports regularly to Senior Leadership Team

Network Manager/Technical Staff:

Novus (managed service provider) are responsible for ensuring:

- That the academy ICT infrastructure is secure and is not open to misuse or malicious attack
- That users may only access the academy's networks through a properly enforced password protection policy
- Technical staff should have no expectations of privacy of academy email accounts, as the e-mails are meant for business communications

Teaching and Support Staff:

Teaching and Support Staff are responsible for ensuring that:

- They have an up-to-date awareness of online safeguarding matters and of the current academy Online Safeguarding Policy and practices
- They have read, understood and signed the school Staff Acceptable Use Policy/Agreement (AUP)
- They report any suspected misuse or problem to the Online Safeguarding Co-ordinator/ Headteacher/Senior Leader/Head of ICT/Class Teacher/Head of Year for investigation/action/sanction
- Staff should have no expectations of privacy of academy email accounts, as the e-mails are meant for business communications
- That passwords are regularly updated
- As staff they must deny current or recent students access to your social media profile so you do not put yourself in a vulnerable position.

Designated person for child protection/Child Protection Officer:

Should be trained in online safeguarding issues and be aware of the potential for serious child Protection issues to arise from:

- Sharing of personal data
- Access to illegal/inappropriate materials
- Inappropriate online contact with adults/strangers
- Potential or actual incidents of grooming
- Cyber-bullying
- Child Protection Officer should have no expectations of privacy of academy email accounts, as the e-mails are meant for business communications

Online Safeguarding Committee:

Members of the online safeguarding Committee will assist the online safeguarding Coordinator and online safeguarding with:

- The production, review and monitoring of the school online safeguarding policy

Students:

- Are responsible for their use of their mobile phones and mobile devices on their 4G network. This should include a knowledge and awareness of risks associated with social media, internet access and video
- In cases, were there has been a suspicion of misuse of mobile devices/phones school staff may request to access contents of the phone/device. We would expect the student to comply.
- Are responsible for using the academy ICT systems and mobile technologies in accordance with the Student Acceptable Use Policy, which they will be expected to sign before being given access to academy systems
- Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Students should have no expectations of privacy of school email account, as the e-mails are meant for school communications
- Are to fully understand the risks posed to children by access to the Internet (see appendix 3)

Parents/Carers:

The academy will take every opportunity to help parents understand these issues through Parents' Evenings, newsletters, letters, website/Learning Platform and information about national/local Online safety campaigns/ literature. Parents and carers will be responsible for:

- Endorsing the Student Acceptable Use Policy
- Accessing the academy ICT systems or Learning Platform in accordance with the academy Acceptable Use Policy.

Community Users:

Community Users who access academy ICT systems or Learning Platform as part of the Extended School provision will be expected to sign a Community User Acceptable Use Policy (AUP) before being provided with access to school systems.

Online Safeguarding Education and Training

Education - Students:

Online safeguarding education will be provided in the following ways:

- A planned online safeguarding programme will be provided as part of ICT lessons and will be regularly revisited – this will cover both the use of ICT and new technologies in and outside school
- Key online safeguarding messages will be reinforced as part of a planned programme of assemblies and tutorial/pastoral activities
- Students will be taught in all lessons to be critically aware of the materials/content they access on-line and be guided to validate the accuracy of information

Education & Training - Staff:

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

- A planned programme of formal online safeguarding training will be made available to staff. An audit of the online safeguarding training needs of all staff will be carried out regularly. It is expected that some staff will identify online safeguarding as a training need within the performance management process.
- All new staff will receive online safeguarding training as part of their induction programme, ensuring that they fully understand the academy online safeguarding policy and Acceptable Use Policies

Communication devices and methods:

The following table shows the academy policy on the use of communication devices and methods.

Where it is indicated that the method or device is allowed at certain times, these are clearly outlined in the next table.

	Staff & other adults				Students			
Communication method or device	Allowed	Allowed at certain times	Allowed for selected staff	Not allowed	Allowed	Allowed at certain times	Allowed with staff permission	Not allowed
Mobile phones may be brought to school	✓				✓			
Use of mobile phones in lessons				✓				✓
Use of mobile phones in social time		✓				✓		
Taking photos on personal mobile phones or other camera devices			✓					✓
Use of personal hand held devices eg. PDAs, PSPs		✓				✓		
Use of personal email addresses in school, or on school network				✓				✓
Use of school email for personal emails		✓						✓
Use of chat rooms / facilities				✓				✓
Use of instant messaging				✓				✓
Use of social networking sites			✓					✓
Use of blogs			✓					✓

This table indicates when some of the methods or devices above may be allowed:

	Circumstances when these may be allowed	
Communication method or device	**Staff & other adults**	**Students**
Mobile phones may be brought to school	Allowed	Allowed
Use of mobile phones in lessons	Emergency situations Head/Deputy	Not allowed
Use of mobile phones in social time	e.g. during breaks or after school	e.g. during breaks or after school
Taking photos on personal mobile phones or other camera devices	Not allowed	Not allowed
Use of personal hand held devices e.g. PDAs, PSPs	Certain times	Certain times
Use of personal email addresses in school, or on school network	e.g. during breaks or after school	Not allowed
Use of school email for personal emails	Not allowed	Not allowed
Use of chat rooms / facilities	Not allowed	Not allowed
Use of instant messaging	Not allowed	Not allowed
Use of social networking sites Linked to school purposes	Certain people	Not allowed
Use of blogs -Linked to school purposes	Certain people	Not allowed

Unsuitable/inappropriate activities:

The academy believes that the activities referred to in the following section would be inappropriate in a school context and those users, as defined below, should not engage in these activities in school or outside school when using academy equipment or systems. The academy policy restricts certain internet usage as follows:

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
User Actions					
Child sexual abuse images					**X**
Promotion or conduct of illegal acts, eg. under the child protection, obscenity, computer misuse and fraud legislation					**X**
Adult material that potentially breaches the Obscene Publications Act in the UK					**X**
Criminally racist material in UK					**X**
Pornography					**X**
Promotion of any kind of discrimination based on race, gender, sexual orientation, religion and belief, age and disability					**X**
Promotion of racial or religious hatred					**X**
Threatening behaviour, including promotion of physical violence or mental harm					**X**
Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute				**X**	
Using academy systems to run a private business				**X**	
Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed by SCC and/ or the academy				**X**	
Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions				**X**	
Revealing or publicising confidential or proprietary information (eg. financial/personal information, databases, computer/network access codes and passwords)				**X**	

	Acceptable	Acceptable at certain times	Acceptable for nominated users	Unacceptable	Unacceptable and illegal
Creating or propagating computer viruses or other harmful files				**X**	
Carrying out sustained or instantaneous high volume network traffic (downloading/uploading files) that causes network congestion and hinders others in their use of the Internet				**X**	
Online gaming (educational)	**X**				
Online gaming (non-educational)		**X**			
Online gambling				**X**	
Online shopping/commerce		**X**			
Use of social networking sites			**X**		
Use of video broadcasting e.g. YouTube			**X**		
Accessing the internet for personal or social use (eg. online shopping)		**X**			
Using external data storage devices (eg. USB) that have not been encrypted (password protected and checked for viruses				**X**	

Good practice guidelines: Email

Best practice

✓ DO

Staff and students should only use their school email account to communicate with each other

Safe practice

Check the academy school online safety policy regarding use of your academy email or the Internet for personal use e.g. shopping

Poor practice

✗ DO NOT

Staff - don't use your personal email account to communicate with students and their families without a manager's knowledge or permission - and in accordance with the online safety policy

Good practice guidelines: Images, photos and videos

Best practice

✓ DO

Only use academy equipment for taking pictures and videos

Safe practice

Check the online safety policy for any instances where using personal devices may be allowed

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the academy network immediately after the event

Delete images from the camera/ device after downloading

Poor practice

✗ DO NOT

Don't download images from organisation equipment to your own equipment

Don't use your own equipment without Headteacher/SLT knowledge or permission - and in accordance with the online safety policy

Don't retain copy or distribute images for your personal use

Good practice guidelines: Internet

Best practice

✓ DO

Understand how to search safely online and how to report inappropriate content

Safe practice

Staff and students should be aware that monitoring software will log online activity.

Be aware that keystroke monitoring software does just that. This means that if you are online shopping then your passwords, credit card numbers and security codes will all be visible to the monitoring technicians

Poor practice

✗ DO NOT

Remember that accessing or downloading inappropriate or illegal material may result in criminal proceedings

Breach of the online safety and acceptable use policies may result in confiscation of equipment, closing of accounts and instigation of sanctions

Good practice guidelines: Mobile phones

Best practice

✓ DO

Staff - If you need to use a mobile phone while on school business (trips etc.), the school will provide equipment for you

Make sure you know about inbuilt software/facilities and switch off if appropriate

Safe practice

Check the online safety policy for any instances where using personal phones may be allowed

Staff - Make sure you know how to employ safety measures like concealing your number by dialling 141 first

Poor practice

✖ DO NOT

Staff - Don't use your own phone without the Headteacher/SLT knowledge or permission

Don't retain service student/parental contact details for your personal use

Good practice guidelines: Social networking (eg Facebook/Twitter)

Best practice

✓ DO

If you have a personal account, regularly check all settings and make sure your security settings are not 'open access'

Ask family and friends to not post tagged images of you on their open access profiles

Safe practice

Don't accept people you don't know as friends

Be aware that belonging to a 'group' can allow access to your profile

Poor practice

✖ DO NOT

Don't have an open access profile that includes inappropriate personal information and images, photos or videos.

Staff: Don't accept students or their parents as friends on your personal profile

•Don't accept ex-student users as friends

•Don't write inappropriate or indiscrete posts about colleagues, students or their parents

Good practice guidelines: Webcams

Best practice

✓ DO

Make sure you know about inbuilt software/ facilities and switch off when not in use

Safe practice

Check the online safety policy for any instances where using personal devices may be allowed

Always make sure you have the Headteacher/SLT knowledge or permission

Make arrangements for pictures to be downloaded to the academy network immediately after the event

Delete images from the camera/device after downloading

Poor practice

× DO NOT

Don't download images from organisation equipment to your own equipment

Don't use your own equipment without Headteacher/SLT knowledge or permission - and in accordance with the online safety policy

Don't retain copy or distribute images for your personal use

Incident Management: Students

Incidents (Students)	Refer to class teacher	Refer to Head of Department / PPC	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction e.g. Correction/ exclusion
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable / inappropriate activities)	✓	✓	✓	✓	✓	✓	✓	✓	✓
Unauthorised use of non-educational sites during lessons	✓	✓						✓	✓
Unauthorised use of mobile phone/ digital camera/other handheld device	✓	✓						✓	✓
Unauthorised use of social networking/ instant messaging/personal email	✓	✓						✓	✓
Unauthorised downloading or uploading of files	✓	✓						✓	✓
Allowing others to access academy network by sharing username and passwords	✓	✓			✓			✓	✓
Attempting to access or accessing the academy network, using another student's account	✓	✓			✓			✓	✓
Attempting to access or accessing the academy network, using the account of a member of staff	✓	✓			✓		✓	✓	✓
Corrupting or destroying the data of other users	✓	✓			✓			✓	✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓	✓		✓	✓	✓		✓	✓
Continued infringements of the above, following previous warnings or sanctions	✓	✓	✓						✓
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	✓	✓	✓	✓	✓	✓	✓	✓	✓
Using proxy sites or other means to subvert the academy's filtering system	✓	✓			✓	✓		✓	✓

	Refer to class teacher	Refer to Head of Department / PPC	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Inform parents/carers	Removal of network/internet access rights	Warning	Further sanction eg. correction/ exclusion
Accidentally accessing offensive or pornographic material and failing to report the incident	✓	✓			✓	✓			
Deliberately accessing or trying to access offensive or pornographic material	✓	✓	✓	✓	✓	✓	✓	✓	✓
Receipt or transmission of material that infringes the copyright of another person or infringes the Data Protection	✓	✓	✓	✓	✓	✓	✓	✓	✓

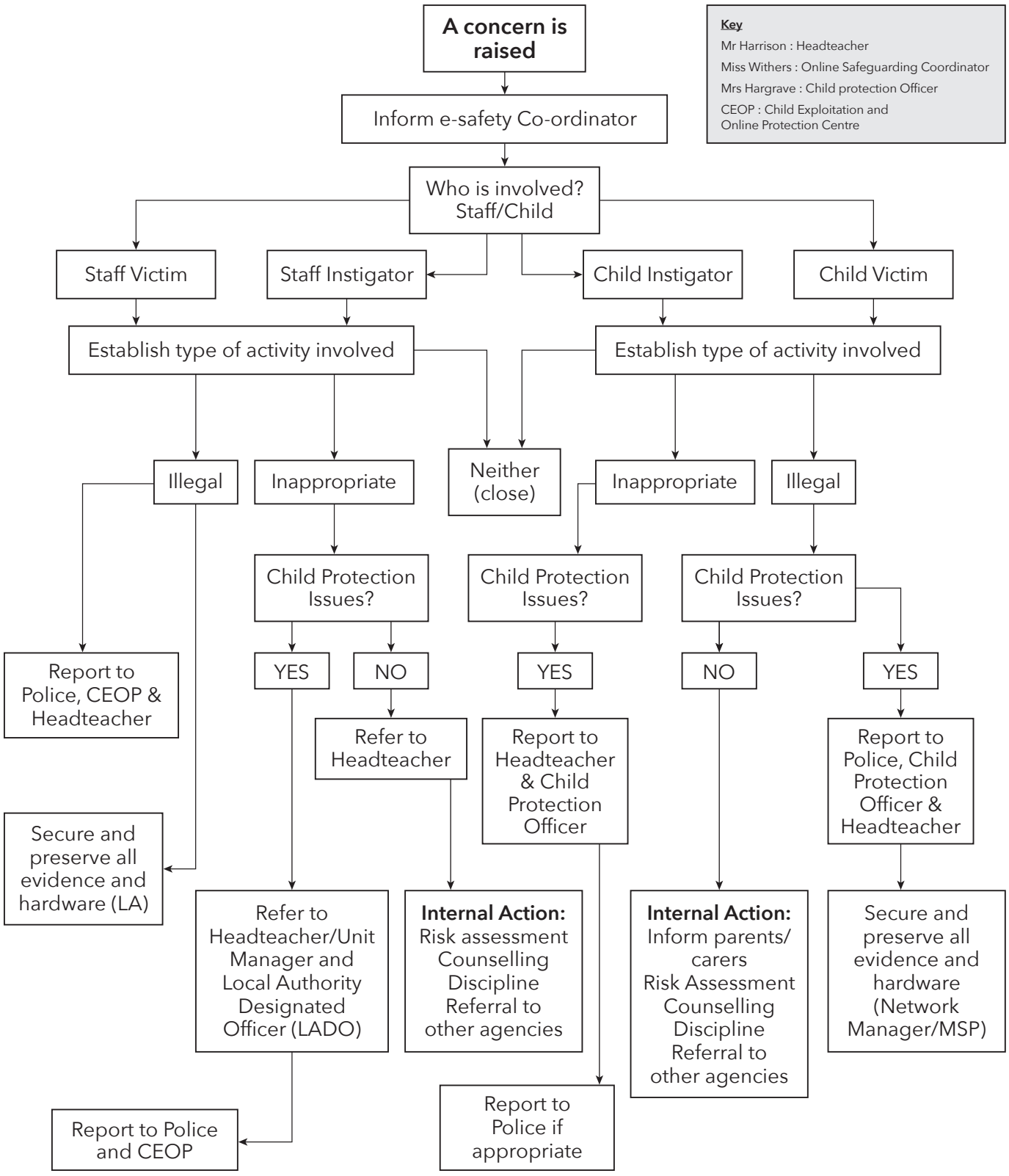
Incident Management: Staff and Community Users

Incidents (Staff & Community Users)	Director of Learning/PPC	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Removal of network/internet access rights	Further sanction (could lead to disciplinary action)
Deliberately accessing or trying to access material that could be considered illegal (see list in earlier section on unsuitable/ inappropriate activities)	✓	✓	✓	✓	✓	✓
Excessive or inappropriate personal use of the Internet/social networking sites/ instant messaging/personal email	✓					✓
Unauthorised downloading or uploading of files						✓
Allowing others to access the academy network by sharing username and passwords or attempting to access or accessing the academy network, using another person's account	✓			✓		✓
Careless use of personal data eg. holding or transferring data in an insecure manner	✓			✓		✓
Deliberate actions to breach data protection or network security rules	✓			✓		✓
Corrupting or destroying the data of other users or causing deliberate damage to hardware or software	✓					✓
Sending an email, text or instant message that is regarded as offensive, harassment or of a bullying nature	✓		✓	✓		✓
Using personal email/social networking/ instant messaging/text messaging to carrying out digital communications with students	✓	✓		✓		✓
Actions which could compromise the staff member's professional standing	✓	✓				✓
Actions which could bring the academy into disrepute or breach the integrity of the ethos of the academy	✓	✓				✓

	Director of Learning/PPC	Refer to Headteacher	Refer to Police	Refer to technical support staff for action re filtering/security etc.	Removal of network/internet access rights	Further sanction (could lead to disciplinary action)
Using proxy sites or other means to subvert the school's filtering system	✓					✓
Accidentally accessing offensive or pornographic material and failing to report the incident	✓			✓		✓
Deliberately accessing or trying to access offensive or pornographic material	✓	✓		✓	✓	✓
Breaching copyright or licensing regulations	✓					
Continued infringements of the above, following previous warnings or sanctions	✓					✓

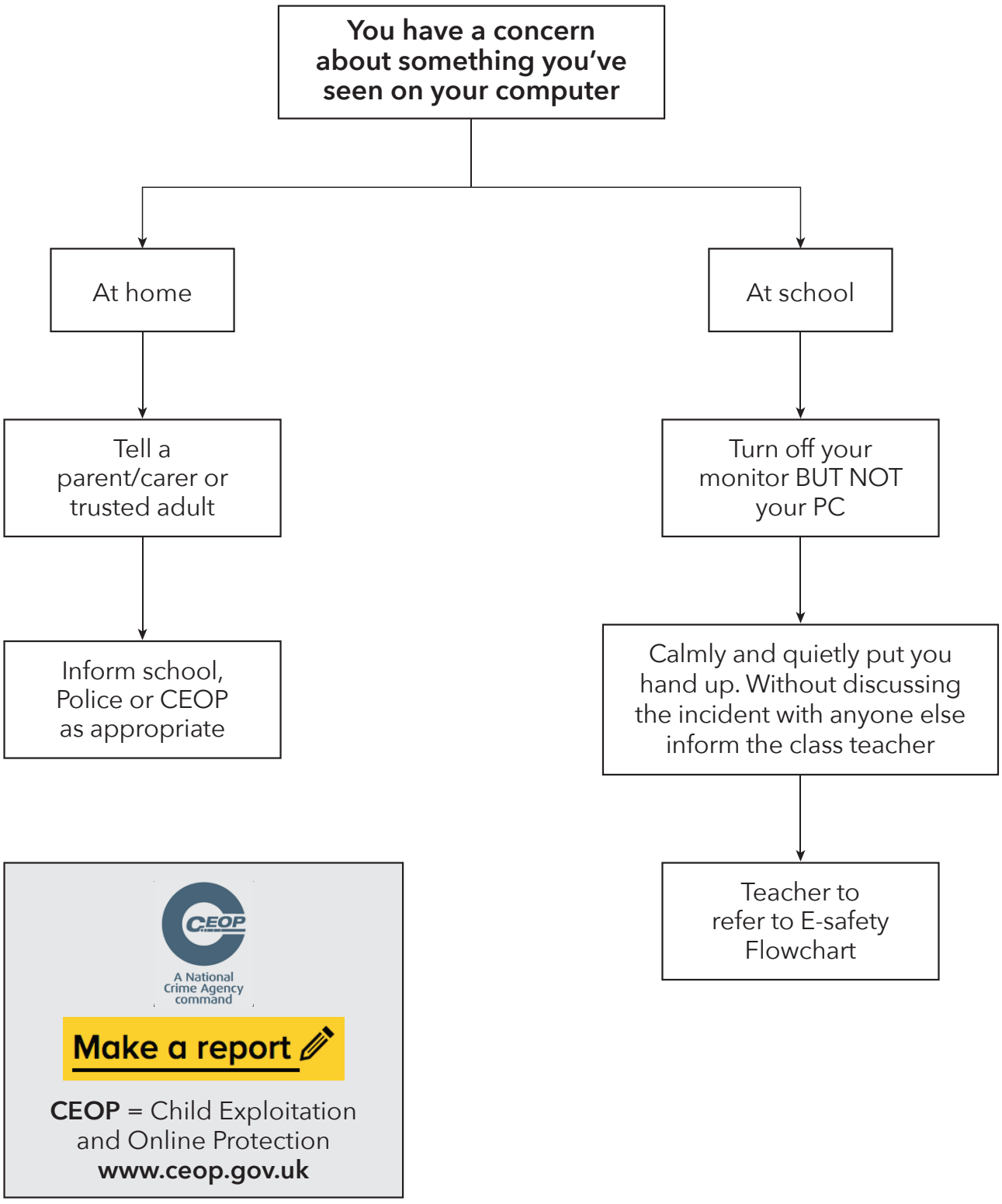
Co-op Academy Swinton

Staff Online Safeguarding Incident Flowchart



Co-op Academy Swinton

Student Online Safeguarding Incident Flowchart



Appendix 1 : Student AUP

Student Acceptable Use Policy Agreement

Please make sure you read and understand the following ☑ **I WILL** and ☒ **I WILL NOT** statements. If there's anything you're not sure of, please ask your teacher.

☑ I WILL

- I will not share my username and password, or try to use any other person's username and password
- Immediately report any unpleasant or inappropriate material or messages or anything that makes me feel uncomfortable when I see it online
- Respect others' work and property and will not access, copy, remove or change anyone else's files, without their knowledge and permission
- Be polite and responsible when I communicate with others, I will not use strong, aggressive or inappropriate language and I appreciate that others may have different opinions
- Only use my personal handheld/external devices (mobile phones/USB devices etc.) in school if I have permission
- Understand that, if I do use my own devices in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment
- Immediately report any damage or faults involving equipment or software, however this may have happened

☑ I WILL NOT

- Try (unless I have permission) to make downloads or uploads from the Internet
- Take or share images (pictures and videos) of anyone without their permission
- Use the academy ICT systems for online gaming, online gambling, internet shopping, file sharing, social networking or video broadcasting (eg. YouTube), unless I have permission of a member of staff to do so.
- Try to upload, download or access any materials which are illegal or inappropriate or may cause harm or distress to others
- Try to use any programmes or software that might allow me to bypass the filtering/ security systems in place to prevent access to such materials
- Open any attachments to emails, unless I know and trust the person/organisation who sent the email, due to the risk of the attachment containing viruses or other harmful programmes
- Attempt to install programmes of any type on a machine, or store programmes on a computer
- Try to alter computer settings

Student Acceptable Use Policy Agreement

This form relates to the Student Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions, both in and out of the academy:

- I understand that the school also has the right to take action against me if I am involved in incidents of inappropriate behaviour, that are covered in this agreement, when I am out of school and where they involve my membership of the school community (examples would be cyber-bullying, use of images or personal information)
- I understand that if I fail to follow this Acceptable Use Policy Agreement, I will be subject to disciplinary action. This may include loss of access to the academy network/internet, corrections, suspensions, contact with parents and in the event of illegal activities involvement of the police
- I understand that I should have no expectations of privacy of academy email accounts, as the e-mails are meant for academy communications

I have read and understand the above and agree to follow these guidelines when:

- I use the academy ICT systems and equipment (both in and out of the academy)
- I use my own equipment in the academy (when allowed) eg. mobile phones, PDAs, cameras etc.
- I use my own equipment out of the academy in a way that is related to me being a member of this academy eg. communicating with other members of the academy, accessing academy email, Learning Platform, website etc.

(Parents/carers are requested to sign the permission form below to show your support of the school in this important aspect of the school's work).

Name of student:		
Group/Class:		
Signed (Student):		Date:
Signed (Parent/Carer):		Date:

Appendix 2 : Staff, Volunteer and Community User AUP

Staff, Volunteer and Community User Acceptable Use Policy Agreement Template

Academy Policy

This Acceptable Use Policy (AUP) is intended to ensure:

- That staff, volunteers and community users will be responsible users and stay safe while using the Internet and other communications technologies for educational, personal and recreational use.
- That academy ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- That staff, volunteers and community users are protected from potential risk in their use of ICT in their everyday work.

The academy will try to ensure that staff, volunteers and community users will have good access to ICT to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff, volunteers and community users to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use academy ICT systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the ICT systems and other users. I recognise the value of the use of ICT for enhancing learning and will ensure that students receive opportunities to gain from the use of ICT. I will, where possible, educate the young people in my care in the safe use of ICT and embed online safety in my work with young people.

For my professional and personal safety:

- I understand that the academy will monitor my use of the ICT systems, email and other digital communications.
- I understand that the rules set out in this agreement also apply to use of academy ICT systems (e.g. laptops, email, VLE etc.) out of the academy.
- I understand that the academy ICT systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the academy.
- I will not disclose my username or password to anyone else, nor will I try to use any other person’s username and password.
- I will immediately report any illegal, inappropriate or harmful material or incident I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.
- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and/or publish images of others I will do so with their permission and in accordance with the academy's policy on the use of digital/video images. I will not use my personal equipment to record these images, unless I have permission to do so. Where these images are published (eg. on the academy website/VLE) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only use chat and social networking sites in the academy in accordance with the academy's policies.
- I will only communicate with students and parents/carers using official academy systems. Any such communication will be professional in tone and manner.
- I will not engage in any online activity that may compromise my professional responsibilities.
- I understand that I should have no expectations of privacy of academy email account, as the emails are meant for business communications

The academy has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the academy:

- When I use my personal hand-held/external devices (PDAs/laptops/mobile phones/ USB devices etc.) in the academy, I will follow the rules set out in this agreement, in the same way as if I was using academy equipment. I will also follow any additional rules in line with the academy's Online safety Policy set by the academy about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses
- I will not use personal email addresses on the academy ICT systems.
- I will not open any attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- •I will ensure that my data is regularly backed up, in accordance with relevant academy policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up Internet capacity and prevent other users from being able to carry out their work.

- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in academy policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself, or others. Where personal data is transferred outside the secure school network, it must be encrypted.
- I understand that data protection policy requires that any staff or student data, to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by academy policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software, however this may have happened.

When using the Internet in my professional capacity or for academy sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work.
- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

Staff, Volunteer and Community User Acceptable Use Agreement Form

This form relates to the Staff, Volunteer and Community User Acceptable Use Policy (AUP), to which it is attached.

I understand that I am responsible for my actions, both in and out of the academy:

I understand that this Acceptable Use Policy applies not only to my work and use of the academy ICT equipment in the academy, but also applies to my use of academy ICT systems and equipment out of the academy and my use of personal equipment in the academy or in situations related to my employment by the academy.

- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include) a warning, a suspension, referral to Governors and in the event of illegal activities the involvement of the police

I have read and understood the academy's Online safeguarding Policy.

I have read and understand the above and agree to use the academy ICT systems (both in and out of the academy) and my own devices (in the academy and when carrying out communications related to the academy) within these guidelines.

Name:	
Position:	
Signed:	
Date:	

Appendix 3 : Use of Images Consent Form

Use of Digital/Video Images

The use of digital/video images plays an important part in learning activities. Students and members of staff may be using digital or video cameras to record evidence of activities in lessons and out of school. These images may then be used in presentations in subsequent lessons.

Images may also be used to celebrate success through their publication in newsletters, on the academy website and occasionally in the press/media.

The academy will comply with the Data Protection Act and request parents/carers permission before taking images of members of the academy.

Parents/carers are requested to sign the permission form below to allow the academy to take and use images of their children.

Parental Consent Form

As an academy we regularly need to request parental consent for a range of issues. We have chosen to implement a combined consent form in order to make the system more efficient. Please find below a summary of issues for which we would now like to request your consent.

Photographs/Digital Images
We need your consent to allow us to use photographs and filmed images of your child on our academy website, social media, academy newsletter and prospectus, local media, video and internal displays around the academy.

Academy Trips/Off-Site Activities
We need your consent for your child to participate in any trips/off-site activities (including residential trips). The academy will send you information about each individual activity before it takes place, allowing you to tell the school whether or not you wish your child to participate.

Emergency Medical Treatment
We need your consent for urgent medical treatment to be given (if required) by a qualified first aider during the academy day or during an out of school activity, where it is not possible to contact you or any other person with parental responsibility.

Internet/ICT Equipment Usage
We need to make you and your child aware of our academy's 'Acceptable Use Agreement' (attached) and online safety policy, please see our website: https://swinton.coopacademies.co.uk/downloads/online safety-policy/.

I understand that my child will be required to sign an Acceptable Use agreement and undertake online safety training to help them to understand the importance of safe use of ICT, both here and home.

Privacy Notice
We need to inform you that we store personal data about you and your child on our school's management systems. We will share this data with the Department for Education and those who provide services to the academy and organisations concerned with the welfare of your child. The privacy notice can be found on our website at: https://swinton.coopacademies.co.uk/downloads/privacy-notice-parents/

Parental Consent Form

NB: Consent given on this form will cover your child for the whole of their time at Co-op Academy Swinton. Should you change your mind at any time please contact us at: info@swinton.coop or on: 0161 794 6215

Parent/Carer to complete this page

Child's Name: .....

Form Group: .....

Consent Details	**Please mark with ✓ or ✗**
Photographs/Digital Images - Level 1 (Un-named) I give my consent for photographs and filmed images of my child to be used for school promotional purposes eg; website, social media, academy newsletter, advertising materials, internal displays and local media but my child must **NOT** be named.	
Photographs/Digital Images - Level 2 (Named) I give my consent for photographs and filmed images of my child to be used for school promotional purposes eg; website, social media, academy newsletter, advertising materials, internal displays and local media and my child's name **MAY** be used to accompany the image.	
School Trips/Off-Site Activities I consent to my child participating in school trips/off-site activities. I understand that I will receive relevant information before any activities take place and will be given the opportunity to withdraw my consent for individual trips/visits.	
Emergency Medical Treatment I consent to my child receiving necessary urgent medical treatment for any injury or illness that may occur during either the school day or out of school activity.	
Internet/ICT Use (see attached Parent/Carer Acceptable Use Agreement) I consent to my child using the internet and school ICT systems including the Learning Platform in line with the Acceptable Use Policy and Online Safety Policy.	
Privacy Notice (https://swinton.coopacademies.co.uk/downloads/privacy-notice-parents/) I have read the academy's privacy notice explaining how we store data on the academy management systems and share this data with those who provide services to the academy and organisations concerned with the welfare of my child.	

Print Name: ..... Parent/Carer

Signature: ..... Parent/Carer

Appendix 3 : Posed risks to children of constant internet access

Inappropriate Material
One of the key risks of using the Internet, email or chat rooms is that young people may be exposed to inappropriate material. This may be material that is pornographic, hateful or violent in nature; that encourages activities that are dangerous or illegal; or that is just age-inappropriate or biased. One of the key benefits of the web is that it is open to all, but unfortunately this also means that those with extreme political, racist or sexual views, for example, are able to spread their distorted version of the world.

Illegal Behaviour
Some young people may get involved in inappropriate, antisocial or illegal behaviour while using digital technologies. Just as in the real world, groups or cliques can form online, and activities that start out as harmless fun, such as voicing an opposing opinion to another member of a chat room, can quickly escalate to something much more serious

Physical Danger
The threat of physical danger is perhaps the most worrying and extreme risk associated with the use of the Internet and other technologies, and is probably the risk most reported by the media.

A criminal minority make use of the Internet and chat rooms to make contact with young people with the intention of developing relationships which they can progress to sexual activity. Paedophiles will often target a child, posing as a young person with similar interests and hobbies in order to establish an online 'friendship'. These relationships may develop to a point where the paedophile has gained the trust in order to meet in person. These techniques are often known as 'online enticement', 'grooming' or 'child procurement'.

Bullying
Cyber Bullying – whether via the Internet, mobile phone or any other method – is another aspect of the use of new technologies that provide an anonymous method by which bullies can torment their victims. While a young person may or may not be in physical danger, they may receive email, chat or text messages that make them feel embarrassed, upset, depressed or afraid. This can damage their self-esteem and pose a threat to their psychological wellbeing.

Divulging Personal Information
Most parents do not allow their children to give out personal information online and around 50% of children acknowledge this. Just under half of 9-19 year old children who go online once a week say that they have given out personal information, such as their full name, age, address, email address, phone number, hobbies, name of their school etc., to someone they met on the internet.
In summary, risks associated with using the internet and digital technologies are often categorised as resulting from content, contact, commerce or culture.

Illegal Activity
Some children and young people may become involved in other equally serious activities. Possible risks include involvement in identity theft or participation in hate or cult websites, or in the buying and selling of stolen goods. The ease of access to online gambling, suicide sites, sites selling weapons, hacking sites, and sites providing recipes for making drugs or bombs are also of great concern. There is some evidence to suggest that young people have become involved in the viewing, possession, making and distribution of indecent and/or child abuse/pornographic images.

Content	Commerce	Contact	Culture
• Exposure to age inappropriate material • Exposure to inaccurate or misleading information • Exposure to socially unacceptable material that might incite violence hate or intolerance • Exposure to illegal material	• Exposure of minors to inappropriate commercial advertising • Online gambling • Commercial and financial scams • Divulging personal information	• Grooming using communication technologies leading to assault of a sexual or other nature	• Bullying via websites, mobile phones etc • Downloading of copyrighted material for example music and films