Internet Safety Policy and Guidelines on Multimedia

INCLUDING GUIDELINES FOR STAFF

This policy has been written with reference to the Byron Report (March 2008) and Safeguarding in a Digital World (CCPAS 2011).
It is informed by the SW Grid for Learning Model Policy
It is to be read in conjunction with the following Wings policies:

- **Safeguarding Policy**
- **Data Protection Policy**
- **Confidentiality Policy**
- **Guidelines for Service Users using electronic media (Appendix 5)**

Introduction

New technology offers extraordinary opportunities but also brings increased risks. The internet poses particular risks because it is ubiquitous and anonymous, and because users act differently on line since there are no gatekeepers or visual cues, something that young people and children find especially complex. Often the same young people who are vulnerable to abuse in the real world will be especially at risk on line and will need more help to become discerning.

It is important that young people are enabled to develop their use of the media in ways that are appropriate to their maturity, and to become discriminating and resilient users.

This policy outlines expectations of staff at Wings in their use of media with young people. Guidelines to help young people develop their own safe use of media are to be found at the end of this Policy (Appendix 1).

Use of social networking sites by workers makes it harder to maintain boundaries in their private life, and also opens up the possibility of relationships between 'friends' who are children and 'friends' who are from the workers' adult personal world.

There are risks both for children and also for workers, who may find images and text appearing on their profiles which can be damaging to their reputations and positions as role models.

Workers should maintain the highest standards of integrity whenever they communicate with young people using text, social networking sites email and other electronic means, as they would face to face.

Contents

Organisation and Management

The Organisation

- Maintains an asset register of all devices and places where personal data is stored.
- Ensures all devices are password protected and media is stored securely
- Maintains Filtering & Monitoring Software on all devices used unsupervised in all educational settings as per KCSiE.
- Passwords are 8 characters minimum and contain lower case and upper-case letters, numeric and special characters
- Ensures that the password for the Admin Computer will be changed if the password is compromised or in the event of staff change.
- Ensures that access to the shared drive via Microsoft Office is controlled via the "Admin" account (controlled by Nominated Officer for Online Safety) and in the event of a potential security breach, the passwords will be reset.
- Ensures antivirus software is installed on all devices.
- Maintains a procedure in case of a breach in data protection (Appendix A)
- Maintains a staff Acceptable Use Policy (Appendix B)
- Maintains a Community Acceptable Use Policy (Appendix C)
- Follows a Safety Incidents Flow Chart see (Appendix D)
- Designates no -mobile -phone areas demarcated with signs
- Ensures clients sign Community Acceptable Use Policy
- Appoints a Nominated Officer for Online Safety who will be responsible for:
    - Ensuring this policy is followed by staff
    - Maintaining the asset register
    - Monitoring incidents
    - Training staff and identified groups of clients
    - Changing the Wi-Fi code if it is believed to be compromised
    - Updating the Policy annually
    - Keeping abreast of changes to internet and social media use

Email

Workers should:

- Use clear, unambiguous language to reduce the risk of misinterpretation (e.g. workers should never use terms such as 'luv' to round things off).
- Ensure all messages can be viewed if necessary, by the worker's line manager.
- Follow the guidelines on confidentiality in the Confidentiality Policy –ie be clear that information disclosed in an email will be shared with others if the young person or others may be at risk of harm.
- Keep messages factual and short – use face to face contact for discussions or mentoring.
- Remember that conversations via email are not essentially private and can be forwarded to others by a young person.
- Never imply a special relationship with the young person.

Mobile phones

Workers should:

- Ensure mobile phones are secure
- Wings shared mobile devices should be accessible to multiple staff to ensure accountability.
- Communications to clients should only be made through shared Wings mobile devices, staff email or Wings social media platforms.
- Save any texts or conversations that raise concerns and show them to the line manager.
- Ensure that any images of children taken on a personal mobile phone are uploaded to the organisations' system and kept securely in a timely manner. Workers should not keep images of children on their mobile phone. Photographs of young people should be taken by mobile phone only to be uploaded to official Wings social media following permission of the individuals (obtained on PIFs) and Wings secure storage. Photos should then be deleted from personal phones after this has happened.
- Only use the Wings shared mobile phone for work purposes, (not personal phones) including taking it on trips and camps. Calls /texts should not be sent after 9 pm (except in an emergency).
- Recognise that text messaging is rarely an appropriate response to a young person in a crisis situation or at risk of harm.

Social networking sites

Workers should

- Not have young people under 18 (or vulnerable adults) linked to their own personal social networking pages/apps if they are involved with or have been met at Wings until at least two years after such service users have ceased to be involved with Wings*.* Those already linked prior to involvement should be removed for this same period.
- Never post photos or personal information of young people/vulnerable adults to their own social media accounts

- Ensure they protect themselves by following recognised guidelines to maintain the privacy of their own personal social media accounts (set as private not public).
- Use the dedicated Wings Social Media pages to contact young people regarding Wings activities. Approved staff are set as Social Media Administrators and are responsible for monitoring. Staff should never use their own Social Media account to respond to messages on the Wings Social Media pages.
- Ensure that no photos or information of young people or vulnerable adults is posted on Wings social media accounts without specific parental/carer consent. Written (preferable) or verbal consent should be obtained from young people/vulnerable adults who appear in photos before they are posted.
- Keep communication short and factual – discussions should be face to face.
- Use an appropriate tone – not over familiar and not to imply a special or exclusive relationship.
- Respect confidentiality as per the Confidentiality Policy and not promise to keep secrets.
- To keep all posts on Wings social media accounts clean, devoid of foul language, inappropriate images/jokes and biased political content.
- Observe a cut off point at 9 pm.
- Save any messages causing concern and report to the line manager.
- Not engage in on-line chat with young people except through designated Wings social media accounts shared by all staff, and ensure messages are not of a personal nature.

Computers and the Internet

The organisation is responsible for protecting children & young people using the internet by installing and upgrading suitable filtering & monitoring software on all computers and laptops used by them and responding to alerts made by their activity.
Young people have access to limited parts of the network – other areas are password protected.

Workers should:

- Ensure that all under 18 users of the internet in Wings buildings have internet permission from parents/carers.
- Monitor the use of the internet and report any abuses.
- Be prepared to give help and advice to young people using the internet during sessions – see guidance for young people.
- Password protect their own laptops to avoid young people accessing confidential information.
- Ensure laptops and other devices are set to automatically lock within 5 minutes
- Ensure that laptops are secure if taken home and are not used by other people

The Wings Website

The organisation is responsible for maintaining and updating the website in accordance with the child protection and data protection policies and the site is monitored by the Website Manager working with the Nominated Officer for Internet Safety.

Workers should:

- Avoid using photos/video of individual young people.
- Use photographs in such a way that young people/vulnerable adults cannot be identified by name or location including when uploaded on official Wings Social Media
- Ensure personal email or postal addresses, landline or mobile phone numbers are not published.

Statement:

The organisation reserves the right to monitor any emails, text messages or other communications sent or received on its equipment, and to delete inappropriate or unauthorised text, images or sound.

A confidentiality clause should be added to the signature of all workers eg:

This email is confidential and intended for use of the intended recipient only. If you have received this email in error, please inform us immediately and then delete it. Unless it specifically states otherwise, this email does not form part of a contract.

Viewing or downloading pornographic images during work time or on a work device, viewing criminal or extremist images at any time or keeping digital photographs of young people outside of the limits in this policy will be regarded as gross professional misconduct.

Appendix A

Data Breach Policy

Rationale

- The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority within 72 hours of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, those individuals must also be informed without undue delay.
- Robust breach detection, investigation and internal reporting procedures must be in place to facilitate decision-making about whether it is necessary to notify the relevant supervisory authority and the affected individuals.
- A record of any personal data breaches must be kept, regardless of whether there is a requirement to notify.
- Data breaches include both confirmed and suspected incidents.

This policy sets out how Wings South West will achieve the above in the event of a data breach.

Personal Data Breach

A personal data breach can be broadly defined as a security incident:

- that has affected the confidentiality, integrity or availability of personal data,
- whenever any personal data is lost, destroyed, corrupted or disclosed,
- if someone accesses the data or passes it on without proper authorisation,
- if the data is made unavailable, for example, when it has been encrypted by ransomware, or accidentally lost or destroyed.

An incident may involve the loss, theft or failure of equipment on which sensitive data is stored e.g. laptop, USB stick, iPad/tablet or paper record.

Reporting a data breach

Once a breach within the organisation is suspected it should be reported to the Data Protection Officer (DPO) who will establish whether a breach has occurred, and whether it is still occurring. The DPO will take any immediate steps to minimise the effect of the breach. When a personal data breach has occurred, the DPO will establish the likelihood and severity of the resulting risk to people's rights and freedoms using Appendix 1. If it is likely that there will be a risk then the DPO will inform the Information Commissioner's Office (ICO). If risk is low or is unlikely there is no requirement to report it; however, the DPO will need to be able to justify this decision, which should be documented.

The DPO will report the breach to the ICO within 72 hours. This may be

(a) by phone to 0303 123 1113 to provide the following information:

- what has happened;
- when and how the DPO found out about the breach;
- the people that have been or may be affected by the breach;
- what is being done as a result of the breach;
- contact details for the ICO
- who else has been told.

Or

(b) online using the template at https://ico.org.uk/fororganisations/report-a-breach/personal-data-breach/

Informing individuals affected.
Individuals will be informed as soon as possible by the DPO if there is a HIGH risk that the impact of the breach will be severe. The threshold of risk is higher for notifying individuals than for notifying the ICO.
The information the DPO will provide to individuals is found at Appendix 2

Third Parties
The DPO, along with the CEO, will consider whether outside agencies such as police, insurance companies or banks should be notified. This may be appropriate if illegal activity has occurred, or whether it might occur as a result of the breach.

Records and review.
A record will be made of the incident, regardless of whether notification was required. See Appendix 1, which helps assess the risk.
Once the incident is contained, the DPO with the CEO and any relevant staff, will evaluate the incident and the response to it. Any necessary changes to policy or procedures will be implemented. Training will be given to staff if necessary.

Further help.
The Information Commissioner's Office operate a helpline on 0303 123 1113, and there is helpful information on the website.

Data Breach Policy Appendix 1

Data Breach Record To be completed by the DPO

Section 1 **Notification of Data security breach**	
Date incident discovered:	
Date(s) of incident:	
Name of person reporting the incident:	
Brief description of the nature of the incident:	
Personal data that may have been placed at risk:	
Any action taken at the time of discovery:	
Section 2 **Assessment of severity**	
The nature of the information lost:	
The amount of information lost. Was this information backed up?	
How will this loss affect the organisation – financially, legally, liability, reputationally:	
How many individuals are involved?	
How sensitive is the data? HIGH RISK personal data relating to: • racial or ethnic origin • political opinions • religious belief • trade union membership • genetics • health • sex life or sexual orientation	

Information that could be used to commit identity fraud • information about personal bank accounts • National Insurance number • Copies of passports or visas Personal information relating to children, young people and vulnerable adults Information relating to work performance, salaries etc	
Section 3 **Action taken**	
Was the breach reported to the ICO? Give date	
Was the breach reported to individuals? Give date	
Were other external stakeholders notified? Give dates	
Was the breach reported to the police? Give dates and any actions required.	
Actions taken by the DPO/CEO, and recommendations made.	

Data Breach Policy Appendix 2
Notification of Individuals affected by a data breach
The nature of the personal data breach must be described, in clear and plain language, and the following information provided:

- the name and contact details of the data protection officer
- a description of the likely consequences of the personal data breach
- a description of the measures taken, or proposed to be taken, to deal with the personal data breach and including, where appropriate, of the measures taken to mitigate any possible adverse effects.

APPENDIX B

Staff Acceptable Use Policy

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

For my professional and personal safety:

- I understand that Wings will monitor my use of the Organisation's digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, phone etc.) outside Wings, and to the transfer of personal data (digital or paper based) outside Wings.
- 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 understand that I should not write down or store a password where it is possible that someone may steal it.
- 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 Wings 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 Organisation's policy on the use of digital / video images. Where these images are published (e.g. on the Wings website or social media pages) it will not be possible to identify by name, or other personal information, those who are featured.
- I will only communicate with students / pupils and parents / carers using official Wings systems. Any such communication will be professional in tone and manner.

- I will not engage in any on-line activity that may compromise my professional responsibilities.
- When I use my own mobile devices (laptops / tablets / mobile phones / USB devices etc) at work, I will follow the rules set out in this agreement, in the same way as if I was using Wings equipment. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses and are password protected.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the security systems in place to prevent access to such materials.
- I will not disable or cause any damage to Wings equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the Data Protection Policy.
- Paper based Protected and Restricted data must be held in lockable storage.

- I understand that data protection policy requires that any staff or learner 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 school 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.

I understand that I am responsible for my actions in and out of the Organisation.

- I understand that this Acceptable Use Policy applies not only to my work and use of Wings digital technology equipment in work, but also applies to my use of Wings systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by Wings.
- 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 or a suspension, and in the event of illegal activities, the involvement of the police.

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

Worker / Volunteer Name: .....

Signed: .....

Date: .....

Appendix C

Community Acceptable Use Policy

I understand that I must use Wings systems and devices in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems, devices and other users. This agreement will also apply to any personal devices that I bring into Wings buildings:

- I understand that my use of Wings systems and devices and digital communications will be monitored
- I will not use a personal device that I have brought into Wings for any activity that would be inappropriate.
- I will not upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, terrorist or extremist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not use any programmes or software that might allow me to bypass the security systems in place to prevent access to such materials.
- I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- I will not access, copy, remove or otherwise alter any other user's files, without permission.
- I will ensure that if I take and / or publish images of others I will only do so with their permission. I will not use my personal equipment to record these images, without permission. If images are published it will not be possible to identify by name, or other personal information, those who are featured.
- I will not publish or share any information I have obtained whilst in Wings on any personal website, social networking site or through any other means, unless I have permission from a staff member.
- I will not, without permission, 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 Wings device, nor will I try to alter computer settings, unless I have permission to do so.
- I will not disable or cause any damage to Wings equipment, or the equipment belonging to others.

- I will immediately report any damage or faults involving equipment or software, however this may have happened.

- I will not open any hyperlinks in emails or any attachments to emails, unless I know and trust the person/organisation who sent the email, or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- 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).
- I understand that if I fail to comply with this Acceptable Use Agreement, the Organisation has the right to remove my access to Wings devices
- I understand that Wings 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 College/School and where they involve my membership of the Wings community (examples would be online-bullying, use of images or personal information).
- I understand that if I fail to comply with this acceptable use agreement, I may be subject to disciplinary action. This could include, but is not limited to, loss of access to the College network/internet, suspensions, contact with parents and in the event of illegal activities involvement of the police.

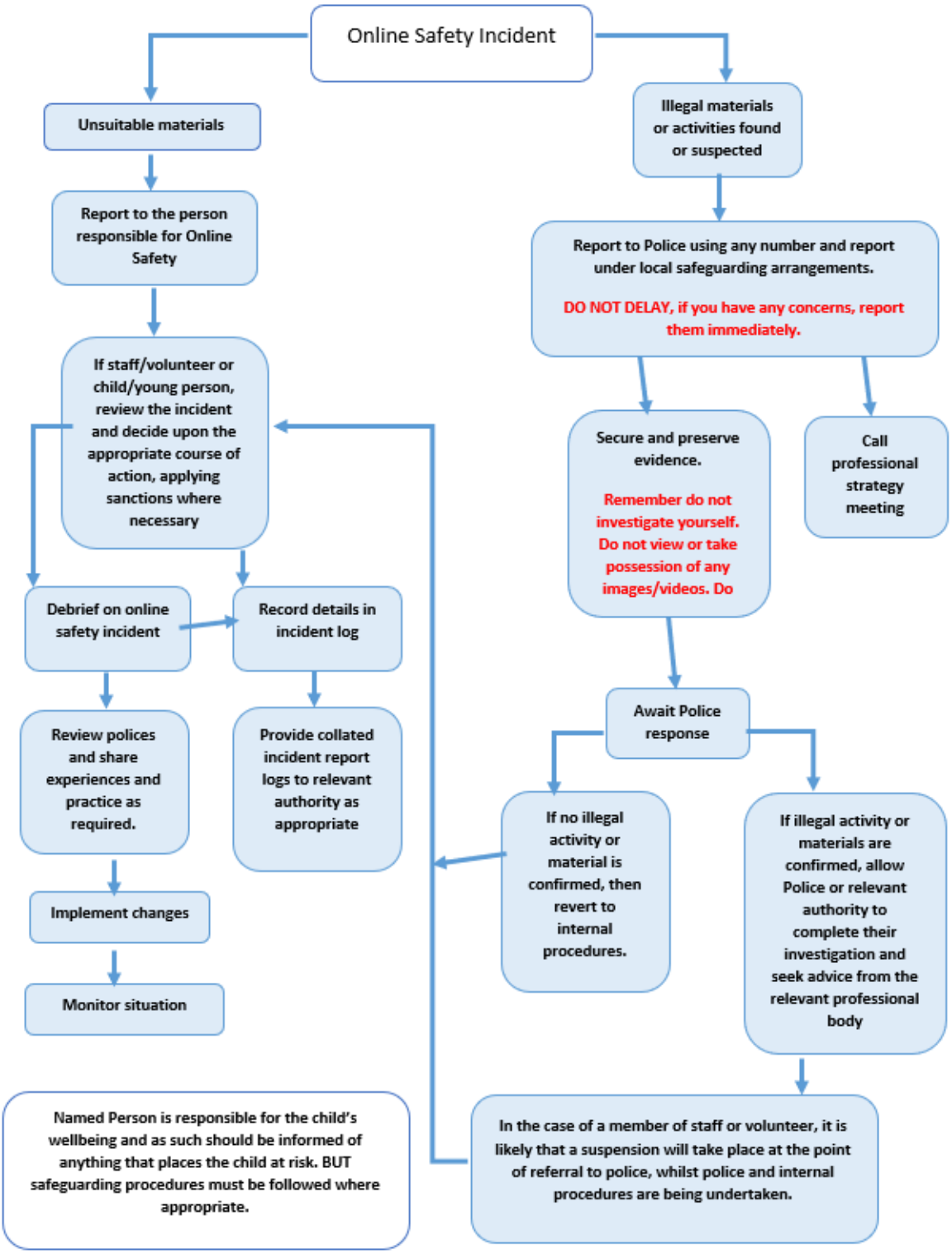
I have read and understand the above and agree to use Wings digital technology systems (both in and out of Wings premises) and my own devices (at Wings and when carrying out communications related to Wings) within these guidelines.

Name: .....

Signed: .....

Date: .....

Appendix D Safety Incidents Flow Chart



It is hoped that all members of the Wings community will be responsible users of digital technologies, who understand and follow Wings 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 the group will need to judge 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
    - Involvement by Local Authority
    - 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
- **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 and demonstrate that visits to these sites were carried out for safeguarding purposes. The completed form should be retained by the Organisation for evidence and reference purposes.

APPENDIX E

Guidance for service users using electronic media

- **risks and advice**

Risks to Young People and Vulnerable adults (service users)

- bullying by peers and people they consider friends.
- exposure to inappropriate and/or harmful content.
- involvement in illegal or inappropriate content.
- posting personal information that can identify and locate a vulnerable person offline.
- theft of personal information.
- sexual grooming, luring, exploitation, radicalisation and abuse through contact with strangers.
- exposure to information and interaction with others who encourage self-harm.
- exposure to racist or hate material.
- encouragement of violent behaviour, such as 'happy slapping'.
- glorifying activities such as drug taking or excessive drinking.
- physical harm to service users in making video content, such as enacting and imitating stunts and risk-taking activities.
- leaving and running away from home as a result of contacts made online.
- involvement in "sexting" with the attendant risk of material considered private being posted on line.
- becoming addicted or over using technology to the detriment of schoolwork or leisure time.
- being dependent on relationships on line rather than in real life.
- pressure to have on line friends and to keep up with trends.

ADVICE FOR STAYING SAFE WHEN USING ONLINE TECHNOLOGY

The discussion of safe use of online technology will be provided for all learners and service users in personal development or mentoring session in line with our RSE policy.

Useful sites for Workers and Young People:

CEOP **The Child Exploitation and Online Protection Centre** **www.ceop.gov.uk**

Thinkuknow **Web resources from CEOP** **www.thinkuknow.co.uk**

Beatbullying **Bullying prevention charity** **www.beatbullying.org**

Cyber Mentors Peer Mentoring on internet safety **www.cybermentors.org.uk**

Childnet **Advice for parents, carers and professionals** **www.childnet-int.org**
KidSmart **Advice from Childnet for young people**
Knowitall **Childnet's resources**

Internet Watch foundation **for reporting abuse** **www.iwf.org.uk**

UK Safer Internet Centre – www.saferinternet.org.uk

UK Council for Internet Safety (UKCIS) - https://www.gov.uk/government/organisations/uk-council-for-internet-safety

South West Grid for Learning - https://swgfl.org.uk/products-services/online-safety/

Professionals Online Safety Helpline - http://www.saferinternet.org.uk/about/helpline

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

Report Harmful Content - https://reportharmfulcontent.com/Harmful Sexual Support Service

NSPCC Removal Tool for explicit images https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/report-remove/