

SWAY – E-Safety Policy

This policy is accepted by SWAY for all projects, groups and activities operating under its banner. All Codes of Conduct, Risk Assessments and Operating Procedures written for any of projects, groups and activities must abide by this policy. It is an obligation, laid down by the Charity Commission that the Board of SWAY ensure that all projects, groups and activities operating in the Charity's name comply with the policy.

1. Introduction

E Safety or Online safety is the collective term for safeguarding involving the use of electronic devices and applications to communicate and access the Internet; often referred to as Information and Communications Technology. This policy covers the safe use of such technology by children, young people, trustees, staff and volunteers in any contexts under the auspices of SWAY.

Many people use mobile phones, e-mail, messaging, video conferencing and other internet applications as an efficient and effective way of communicating. There are a number of concerns which SWAY has in respect of the potential dangers of communicating electronically and use of the internet.

It is therefore appropriate that SWAY has a policy applicable to all its employees at all levels that use the internet and electronic devices so that everyone is aware of the procedures to be used.

2. The Policy

Responsibility for the implementation of this policy lies with the relevant trustees, but some aspects may be delegated to others. Workers refers to all those who work for SWAY in either employed or voluntary roles.

a. General Principles

Trustees of SWAY or those delegated responsibility will:

- Exercise our right to monitor the use of all our systems with internet access. This will include access to websites, the interception of e-mail and the deletion of inappropriate material where we believe unauthorised use of the computer system is or may be taking place, or the system is or may be being used for a criminal purpose or for storing unauthorised or unlawful text, images or sound
- Ensure that unwanted/unsolicited information, viruses and other malware does not intrude on the use of IT
- Ensure all appropriate and reasonable steps are taken to protect computers and the users of them

Workers will:

- Ensure all use of IT is carried out with integrity, appropriately and within the parameters of this policy
- Ensure that all e-communication, is clear and appropriate to the context and purpose and is open to scrutiny
- Be circumspect in all e-communications with children, young people and vulnerable adults, to avoid any possible misinterpretation
- Only give personal details to children, young people and vulnerable adults that are within the public domain and appropriate to the context
- Only make contact with children, young people and vulnerable adults for reasons related to their work and maintain a log of all electronic contact with individuals or groups
- Only use SWAY equipment to communicate for work purposes with children, young people or vulnerable adults, (i.e. not personal equipment) unless previously agreed with trustees or delegated manager
- Only use agreed methods of communication, approved by trustees or delegated manager, and parents/carers
- Respect a person's right to confidentiality unless abuse/harm is suspected or disclosed
- Ensure SWAY's name appears with every Internet post made by a user in the context of their connection to SWAY. Any user may thus be viewed as a representative of SWAY while conducting business on the Internet. No anonymous messages should ever be sent in the work context • Inform parents/carers of intended methods and context of communication and the rules for appropriate use of SWAY equipment and internet use by both workers and children, young people or vulnerable adults. If the parent/carer requests their child is not communicated with in a certain way, this must be respected and an alternative found
- Refer all safeguarding concerns/allegations arising from e-communication to their Safeguarding Officer
- Only communicate with children, young people or vulnerable adults and their parents/carers during reasonable working hours except in emergency circumstances or where there a potential risk of harm. Communication with children and young people should be done within agreed, reasonable hours, for example, taking into account an appropriate bed time for that age and should not take place outside of these times, except in emergency situations.

b. Acceptable Use

When using a computer or electronic device with internet access on SWAY premises, at a SWAY event and/or using SWAY equipment; workers are not permitted to:

- Search for and/or enter inappropriate websites; including pornographic, racist or hate motivated content.
- Send, display, retrieve or copy offensive messages or pictures, unless handling this information is for specific safeguarding/reporting purposes.
- Use obscene language.
- Violate copyright laws; i.e. illegally copy or play copyrighted content where

- permission has not been given.
- Trespass in others' folders, work or files (i.e. enter without permission).
 - Harass, insult, bully or attack others.
 - Damage computers, computer systems or computer networks.
 - Use another user's password.
 - Use equipment or devices without relevant permission or add software without permission.
 - Use computers for unapproved commercial purposes.
 - Access, download, send or receive any data (including images), which are considered offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.

In addition, workers must report anything that is seen or received which may be unsuitable, offensive or which contravenes any of the rules outlined in this policy. Violations of any of these rules could result in disciplinary action being taken in line with SWAY's disciplinary policy. When applicable, police or local authorities will be informed.

Responsible use of equipment belonging to SWAY and the appropriate use of the internet at SWAY activities should also be included on general registration and/or consent forms so that parents/carers understand the rules above and agree that children, young people and vulnerable adults are also subject to these rules whilst participating in activities.

Whilst it is not possible to legislate for how a child, young person or vulnerable adult uses their personal devices, it should be clear that violations of the above rules will have consequences. Serious violations could include a temporary or permanent ban from the activity or group and information being passed on to their parent/carer, the police or other statutory agencies. Some violations could include a ban on use of SWAY equipment or other appropriate sanctions, determined by the local context.

c. Email communication

When communicating via email, every effort should be made to ensure that the method of communication is secure (e.g. only sending email to secure addresses), only accessed by the appropriate person (blind copy or undisclosed recipients function should be used so as not to disclose email addresses to a wider group where not appropriate) and that minimal identifying detail is included where security cannot be guaranteed (e.g. using initials rather than full names).

When using email to communicate with children, young people or vulnerable adults, workers will:

- Ensure all emails are transparent and open to scrutiny. This means they could be viewed at any time by a supervisor or trustee. (Where necessary this should be explained to children and young people, in the same way that confidentiality is not promised in other contexts.)

- Obtain parental agreement before they use email services to communicate with a child or young person.
- Use clear, unambiguous language to reduce the risk of misinterpretation.
- Not give their personal contact details to children or young people, including details of any blogs or personal websites unless these are agreed forms of communication.
- Retain secure records of email communication with children, young people and vulnerable adults, which should be dated.

d. Social Media

Workers will:

- Not use a personal account, in preference to specifically established group accounts or an individual work account, for the purpose of communicating via social media. Not share personal information with a child, young person or vulnerable adult in their care.
- Ensure that administrative details are not shared with children, young people or vulnerable adults.
- Limit interaction with children, young people or vulnerable adults to monitored/administrated groups.
- Ensure that all text and any other media posted shall be subject to the acceptable use rules above.
- Record all interaction on social media groups for safeguarding purposes.
- Only use private messaging in emergency circumstances and never use any non-recordable private messages.
- Ensure all users of social media are above the relevant minimum age limit i.e. 13 for Facebook. (*Reference: Elim Limitless Safeguarding OnLine Guide: Social Media*)
- Ensure their privacy settings offer the highest levels of security in order to restrict children or young people being able to see any more than what is relevant to communication within the group.
- Provide links on social media groups to statutory authorities such as CEOP, to enable children to report online abuse.
- Encourage children, young people and vulnerable adults to use social media responsibly and safely.

e. CYP Use of Internet

CYP access the internet through a restricted access user account. The account is password protected and is only able to be adjusted by the Network Administrator. A log of all sites visited is available. At no time will groups of CYP be using the system unsupervised.

Where they are working on the CYP sites of SWAY's Website all work is checked before being sent live to the website. Any incoming mail for the CYP as a result of website activity is checked before it is viewed.

f. Mobile phones

It is advisable that a worker be supplied with a work-dedicated phone. This way all calls and texts can be accounted for via an itemised phone bill. It also protects the worker's right to a personal life outside work and offers a greater level of accountability and transparency for all concerned.

Where this is not possible, or the work phone is not working or is otherwise unusable, then the worker may use a personal phone for work purposes, within parameters which are agreed in advance with their trustees or delegated manager.

Workers will:

- Ensure all texts and records of phone calls are transparent and open to scrutiny. This means they could be viewed at any time by a supervisor or trustee. (Where necessary this should be explained to children and young people in the same way that confidentiality is not promised in other contexts.)
- Be clear to children, young people and adults at risk of harm of their normal working hours and when they can be available to speak to on the phone or respond to texts.
- Not divulge their personal mobile number unless to ensure contact can be made in exceptional circumstances. These should be reported.
- Use group text rather than texting individuals. Any texts to an individual should be avoided but where necessary, should either be copied to an appropriate colleague or trustee, or otherwise kept and recorded.
- Ensure they use clear, appropriate and unambiguous language and be cautious about the use of emoticons which could be misinterpreted.
- Ensure that any texts or conversations that raise concerns are saved/recorded (either literally or notes made immediately following a conversation) and reported to the worker's supervisor.

- Only make contact via text or mobile calls during set appropriate hours and only for work purposes.
- Enable a password/lock on their phone for data protection and not allow unauthorised access.
- Ensure that they only take photographs of children and young people on their phones in accordance with the guidelines on photography and should not retain copies of images on their work phone, unless previously agreed with their line manager and permission given by parents/carers for this practice. They should never take or store photos of children/young people known through work on their personal phone, unless this is being used in an emergency and photographic evidence needs to be recorded.

g. Chat & Messenger Services

Instant or Direct Messenger Services (IM/DM) are programmes that allow people to write and receive messages in real time and are often used by children and young people for one-to-one or group conversations. The same protocols for workers communicating via email and mobile phone also apply to IM/DM in that care needs to be taken with regard to language and content as well as when and for how long a communication lasts. Workers should ensure that all communications using IM/DM services adhere to the rules above relating to appropriate hours for communication, saving and recording communication and ensuring communication is appropriate and open to scrutiny.

Workers must ensure that they enable settings when using IM/DM services which allow for conversations to be saved as text files and should never use programmes or apps which do not allow conversations to be saved. Children/young people and parents/carers should also be made aware that conversations will be recorded and kept on file.

h. Video Chat

Webcams and phone cameras which allow for the use of programmes such as Zoom, Skype or Facetime mean that individuals or groups can contact one another in real time by using 'video-calling'. These applications are ideal for one-to-one calls or group contacts, where face-to-face meetings are not possible but the same rules must apply, as if meeting physically face-to-face.

Virtual meetings must adhere to the same rules regarding appropriate boundaries, consent, recording and reporting as would be expected from any other meeting or communication outlined above. Workers should not make or receive video chat requests without prior notice, planning or approval.

In order to minimise risks, always consider whether a group communication can be achieved rather than one to one. Where a one to one video call is required it is good practice where possible to have an additional colleague in the room with the worker and (dependent on the age of the young person) also better to ask if

a parent can be in the home of the young person at the same time. Recordings of group calls should not be made unless there is a compelling reason to do so. Note that a Zoom meeting will auto record and will be stored on the cloud. They'll only be accessed if there is a safeguarding disclosure or accusation.

Therefore, workers will:

- Ensure that parental permission is given for group and one-to-one video chats, including the purpose, dates, times and locations for those involved. It is possible to seek consent for regular, adhoc video chats, by outlining the purpose and appropriate boundaries and ensuring these are adhered to.
- As in normal circumstances, unless unavoidable, contact with young people should take place with appropriately vetted and checked workers present and not by any single worker on their own.
- Ensure the call organiser has planned ahead and has the ability to mute/block participants in the event they are displaying/sharing anything unsuitable or illegal.
- If available (eg Zoom) always use a meeting password and turn Waiting Room ON. This feature is also ESSENTIAL to tackling unwanted visitors and also gives you access to the meeting before the guests.
- When participating in online groups or interactions, for example respectful modes of behaviour and speech, appropriate physical presentation such as clothing, venue, environment, locations and times must be considered. 'Break Out Rooms' need supervising too.
- Ensure that all video calls are made at times which are appropriate to the context and age of the child.
- Respect the minimum age requirements for video chat enabled platforms and consider a minimum age limit for any one-to-one chat.
- Avoid using personal accounts to enable video chats. Use organisational profiles and devices wherever available.
- Ensure a record is kept of all one to one video calls held and the content covered in each call. If you intend to record these calls in place of the usual safer working arrangements, ensure that permission has been sought and the recording is stored securely in line with your usual safeguarding protocols.
- Ensure that children/young people understand the risks and dangers of this context, and that it is a not a safe environment to engage in with strangers.
- All CYP are informed how to report anything they are concerned about with regards to behaviour of a worker toward them. SWAY also ensures that parents are aware of who the Safeguarding Officer is in order to discuss any concerns.

(Reference: Elim Limitless - Keeping Safe on Zoom March 2020)

i. Photographic images and film

Working with children and young people may involve the taking or recording of images. Any such work should take place with due regard to the law and the need to safeguard the privacy, dignity, safety and well-being of children and young people. Informed written consent from parents or carers and agreement, where possible, from the child or young person, should always be sought before an image is taken for any purpose. Where images are to be used in any form of publication (including online), express permission must be sought from parents/carers. Clear guidelines must be operated when using images of children and young people and these guidelines apply to all content, be it still photographs, films or audio clips which count as personal data. The following rules apply:

- Workers will ensure there is permission from parents/carers and, where appropriate, the child or young person themselves before any images are taken or displayed.
- Written consent will specify what purposes the image will be used for and how it will be stored. Images will only be used for the specific purpose agreed.
- Written consent will be stored securely and notice given to those responsible for taking images where consent is not given or withdrawn. Workers are responsible for knowing where permission is refused, withdrawn or otherwise not given and will respect this for the relevant child or young person.
- Any worker will be able to justify images of children or young people in their possession using the above clear purpose and no images will be taken for personal use or on personal devices.
- Workers will ensure that children and young people understand why the images are being taken.
- No pictures or film should be taken when anyone is not appropriately dressed or is in any vulnerable situation (unless using as photographic evidence of an injury or abuse).
- Photographs will not enable individual children to be clearly identified, unless specific permission has been given for use.
- Children's full names will not be used anywhere in association with photographs, without permission.
- Use of images will reflect the diversity of age, ethnicity and gender of the activity.
- Live streaming of events must be clearly advertised in advance and where children are involved permission should be sought in line with the photographic guidelines.
- There will be an agreement as to whether the images will be destroyed or retained for further use, where these will be stored and who will have access to them.
- Messages of a suggestive nature must not be sent.
- CYP are not permitted to post images or photo of Charity activities on to the

internet i.e Facebook, Twitter, Snapchat, tumblr etc.

j. Indecent Images

Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and the individual being barred from working with children and young people, if proven. Workers should ensure that children and young people are not exposed to any inappropriate images or web links and will ensure that all IT equipment and devices used have the appropriate controls with regards to access, e.g. personal passwords should be kept confidential. Where indecent images of children or other unsuitable material are found, the process for reporting concerns outlined in the Safeguarding Policy should be followed.

k. 'Sexting'

Sexting refers to sending or receiving indecent or inappropriate images, which can be sent to or from a friend, boyfriend/girlfriend or stranger and although it usually refers to sending via text message, they can also be sent via email, in instant messages or in social media apps etc.

All workers should be aware of the implications of this behaviour. While the age of sexual consent is 16, the relevant legal age in relation to indecent images is 18. It is therefore:

- Illegal for anyone under 18 to send such an image to anyone else, including if the image is of themselves and sent to a 'partner'.
- Illegal for anyone over 18 to send such images to anyone under 18.
- Illegal for anyone of any age to forward on or publicise such images from other people, in any context.
- Illegal for anyone of any age to possess, take, make, distribute or show anyone an indecent image of anyone under 18 years of age.
- Not illegal if sent between consenting adults (but could be considered harassment if unwanted).
- Not illegal if image of an adult is sent between under 18s (but may be referred to social services).

In any of the above contexts, if a worker observes or suspects this behaviour in others, or if this relates to their own behaviour, then this must be reported to their line manager or Safeguarding Officer.

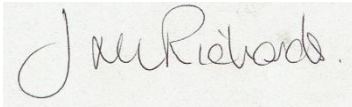
3. Verification

Effectiveness of this policy will be evaluated annually by the Chair of Trustees in conjunction with SWAY staff and the Board through analysis of any issues arising from any transgressions.

4. Revision History:

The Chair of South Wight Area Youth Partnership Board of Trustees will ensure that the policy is reviewed annually or as required by legislation. Any policy that is changed will be brought before the SWAY Board for acceptance to ensure we comply with current legislation and impact assessed against the equality categories.

SWAY-E Safety Policy

Date approved	
Date reviewed	April 2023
Signed	 (Chair of Trustees)
Minuted	
Date of next review	April 2024