E-safety: Policy Statement

Contents

1 Introduction

The most important part of youth work is keeping young people safe. Regardless of why young people engage with our services, there is an expectation from members, parents and guardians, funders, our sector, and local, national and international communities that we keep young people safe.

Mary's (St Mary Islington Community Partnership) is a registered charity that runs a Youth Club and provides training activities related to youth work and community development.

The purpose of this policy statement is to ensure the safety and wellbeing of children and young people is paramount when adults, young people or children are using the internet, social media or mobile devices and provide staff and volunteers with the overarching principles that guide our approach to online safety. As an organisation, we operate in line with our values and within the law in terms of how we use online devices.

The policy statement applies to all staff, volunteers, children and young people and anyone involved in Mary's activities.

1.1 Legal framework

This policy has been drawn up on the basis of legislation, policy and guidance that seeks to protect children and young people in England. Summaries of the key legislation and guidance are available on:

- online abuse learning.nspcc.org.uk/child-abuse-and-neglect/online-abuse
- bullying learning.nspcc.org.uk/child-abuse-and-neglect/bullying
- child protection learning.nspcc.org.uk/child-protection-system

1.2 We believe that:

- children and young people should never experience abuse of any kind
- children and young people should be able to use the internet for education and personal development, but safeguards need to be in place to ensure they are kept safe at all times.

1.3 We recognise that:

- the online world provides everyone with many opportunities; however it can also present risks and challenges
- we have a duty to ensure that all children, young people and adults involved in our organisation are protected from potential harm online
- we have a responsibility to help keep children and young people safe online, whether or not they are using Mary's network and devices
- all children and young people, regardless of age, disability, gender reassignment, race, religion or belief, sex or sexual orientation, have the right to equal protection from all types of harm or abuse
- working in partnership with children, young people, their parents, carers and other agencies is essential in promoting young people's welfare and in helping young people to be responsible in their approach to online safety.

1.4 Named person's role and responsibilities

It is the role of the Designated Safeguarding Lead (DSL) to act as a source of support and guidance on all matters of child protection and safeguarding within the setting. In the absence of the DSL, staff should report any concerns to the Deputy Safeguarding Lead who will report back to the DSL.

2 We will seek to keep children and young people safe by:

- providing clear and specific directions to staff and volunteers on how to behave online through our behaviour code for adults set out in the staff handbook
- supporting and encouraging the young people using our service to use the internet, social media and mobile phones in a way that keeps them safe and shows respect for others
- supporting and encouraging parents and carers to do what they can to keep their children safe online
- developing an online safety agreement for use with young people and their parents/carers (See Appendix No.2 on Acceptable Use Agreements for Staff and Volunteers and different age children)
- developing clear and robust procedures to enable us to respond appropriately to any incidents of inappropriate online behaviour, whether by an adult or a child/young person
- reviewing and updating the security of our information systems regularly
- ensuring that user names, logins, email accounts and passwords are used effectively
- ensuring personal information about the adults and children who are involved in our organisation is held securely and shared only as appropriate
- ensuring that images of children, young people and families are used only after their written permission has been obtained, and only for the purpose for which consent has been given
- providing supervision, support and training for staff and volunteers about online safety
- examining and risk assessing any social media platforms and new technologies before they are used within the organisation.
- Mary's will filter all internet devices to ensure safe access for all Mary's users. See Appendix No. 5

3 If online abuse occurs, we will respond to it by:

- having clear and robust safeguarding procedures in place for responding to abuse (including online abuse see our Safeguarding Policy and Procedures)
- providing support and training for all staff and volunteers on dealing with all forms of abuse, including bullying/cyberbullying, emotional abuse, sexting, sexual abuse and sexual exploitation
- making sure our response takes the needs of the person experiencing abuse, any bystanders and our organisation as a whole into account
- reviewing the plan developed to address online abuse at regular intervals, in order to ensure that any problems have been resolved in the long term.
- All E-Safety incidents will be reported in accordance with Mary's Safeguarding policy

4 Risks and issues

The following are the range of technologies young people and staff/volunteers use positively but which can also put them at risk:

- Internet
- E-mail
- Instant messaging Blogs
- Podcasts
- Social networking sites
- Chat rooms
- Gaming Sites
- Mobile phones with camera and video functionality
- Mobile technology (eg games consoles) that are internet ready and include webcams
- E-smart phones with e-mail, web functionality, camera and video functionality and secure text network

Risks can occur under the categories outlined below:

	Commercial	Aggressive	Sexual	Values
Content That the user may come across either accidentally or via a deliberate search	Adverts Spam Sponsorship Requests for personal information Exposure to age-inappropriate material	Violent/hateful content	Exposure to illegal material, eg, images of child abuse Pornographic/ unwelcome sexual content	Bias Racist Misleading information/ advice

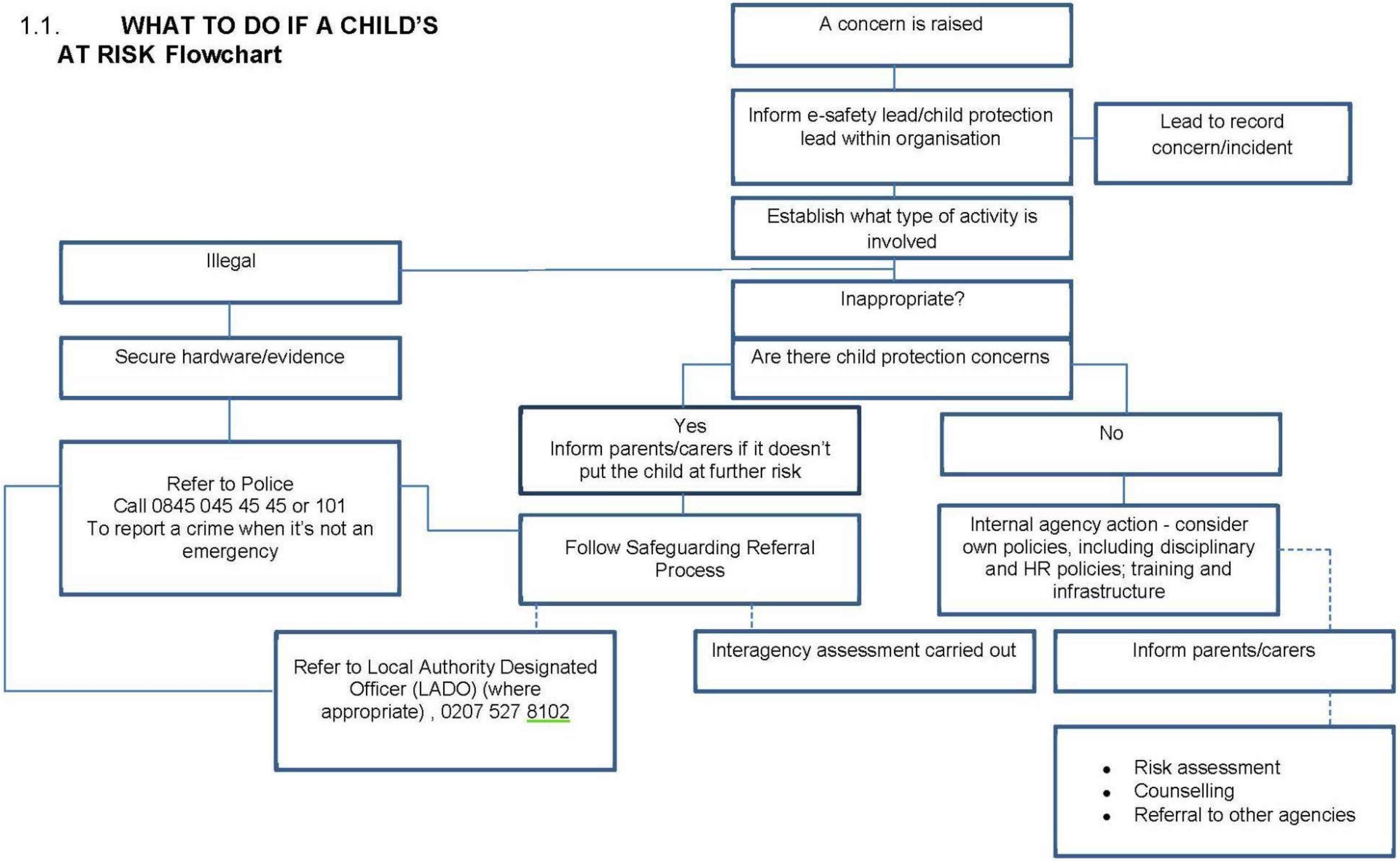
Contact Unsuitable contact from another user	Tracking Harvesting Publishing information about themselves	Being bullied, harassed, stalked	Meeting strangers Being groomed	Self-harm Unwelcome persuasions
Conduct User’s behaviour that creates risk either through illegal activity or lack of awareness of the potential consequences	Illegal downloading Gambling Hacking Financial scams	Bullying or harassing another	Creating and uploading inappropriate / abusive material ‘Sexting’	Providing misleading information/ advice

5 Procedures

All staff and volunteers should be familiar with the leaflet **What to do if you’re worried a child is being abused**. (HM Government, March 2015) and Mary’s whistle-blowing procedures. If you are concerned that a child may be at risk, follow the What to do if a Child or Young Person is at Risk flowchart in this document.

5.1 What to do if a Child or Young Person is at Risk

1.1. WHAT TO DO IF A CHILD'S AT RISK Flowchart



A concern is raised

Inform e-safety lead/child protection lead within organisation

Lead to record concern/incident

Establish what type of activity is involved

Illegal

Secure hardware/evidence

Refer to Police
Call 0845 045 45 45 or 101
To report a crime when it's not an emergency

Inappropriate?

Are there child protection concerns

Yes
Inform parents/carers if it doesn't put the child at further risk

Follow Safeguarding Referral Process

Refer to Local Authority Designated Officer (LADO) (where appropriate) , 0207 527 8102

Interagency assessment carried out

No

Internal agency action - consider own policies, including disciplinary and HR policies; training and infrastructure

Inform parents/carers

- Risk assessment
- Counselling
- Referral to other agencies

5.2 E-Safety Tips for Mary's Delivery Team

- Set your privacy setting to "Just Friends" so that your details, photographs, location, etc can only be seen by your invited friends.
- Have a neutral picture of yourself as your profile image. Don't post potentially embarrassing material.
- Reject or ignore friendship requests unless you know the person or want to accept them. Choose your social networking friends carefully and ask about their privacy controls.
- Do not accept 'friendship requests' on social networking or messaging sites from children/young people (or their parents) that you work with.
- For groups and networks set your privacy setting to private or everyone in the group or network will be able to see your profile.
- If you wish to set up a social networking site for a work project create a new user profile for this. Do not use your own profile.
- Use location settings wisely. Many social networking and online applications disclose your location. Where this is specifically linked to your identity it will, within a couple of days have disclosed where you live and when you are not at home.
- There are social networking groups to bring together people sharing experiences, such as attending festivals and conferences. This advertises when you will not be at home.
- Be careful not to leave your Facebook account logged-in in a shared area/household. Someone could leave status messages that may compromise or embarrass you. This is called Frape (Facebook Rape) and can be a form of cyber-bullying.
- If you think someone is impersonating you on Facebook or similar, report it. Impersonation usually breaches the terms and conditions – you will need to know the specific URL or user name
- Think before you post. Once something is on the internet, even if you remove it, the chances are it has already been snapshotted by a "web crawler" and it will always be there.
- Be aware of addictive behaviour. Adults are just as likely as young people to get hooked on social networking, searching or games.
- When you log-into a web site, unless your computer is exclusive to you, do not tick boxes that say 'remember me'.
- Do not leave yourself logged into your computer, software or websites. If you have to move away from your computer, log out.
- Use strong passwords that include a mixture of upper and lower case letters, numbers and other characters, are a minimum of 8 characters in length and do not contain the person's username. Do not to use the 'Remember Password' feature of applications.
- Turn Bluetooth off when you are not using it. If you open un-pass worded Bluetooth anyone with Bluetooth in range can read the content of your phone or device.
- Lock your mobile. Set a pin number or password for your mobile phone. With access to email, social networking and contacts an unlocked mobile phone can put your identity, and others, at risk.

5.3 Young People's Acceptable Use Agreements

These rules and guidance apply to our computers, our networks (including wifi) and personal devices while on our premises or taking part in our activities.

Members must not:

- Use the internet or email for the purposes of harassment, abuse or illegal activities.
- Use or share profanity, obscenities, or derogatory remarks in communications.
- Access, download, send or receive any data (including images), which Mary's considers offensive in any way, including sexually explicit, discriminatory, defamatory or libellous material.
- Use the internet or email to gamble.
- Use the email systems in a way that could affect its reliability or effectiveness, for example distributing chain letters or spam.
- Download copyrighted material such as music media (MP3) files, film and video files (not an exhaustive list) without appropriate approval.
- In any way infringe any copyright, database rights, trademarks or other intellectual property.
- Download any software from the internet without prior approval of Mary’s Staff.
- Connect personal devices to Mary’s Computers.
- Report any faults or issues with Mary’s Equipment
- Follow the Stay Safe Online Guidance below

Stay Safe Online Guidance

- Keep your personal information safe.
- Protect your passwords.
- Remember that not everyone online is who they say they are!
- Tell a parent or staff member about any meetings you are planning with someone you have communicated with only online.
- Never open emails from people that you don’t know.
- Check your privacy settings to make sure only the people you want see your information and photographs.
- If you use social networking sites, remember that it’s not a game to add as many people as you can to look more popular.
- Think carefully before uploading photos.
- If you see anything on the internet that makes you feel uncomfortable, tell a member of staff.

5.4 Control Procedures of Mary’s Use of ICT to Ensure Safety of Users

5.4.1 Internet

Internet access at St. Mary’s Neighbourhood Centre is provided by St Mary’s Islington Church.

5.4.2 Email

E-mail accounts require 2 step verification process for log in preventing access from unauthorised devices by unauthorised users.

Mary’s will use standard email addresses. MARY’S will provide staff and volunteers with an email account for their professional use. These e-mail accounts are subject to pre-set security policies controlled by Mary’s.

5.4.3 Digital and video images

We obtain written parental/carer permission for use of digital photographs or video involving their child as part of the agreement form when their child joins Youth Club.

Recordings of young people are stored in a securely on the organisations systems and deleted when no longer required for the permitted purpose they were taken for.

We do not identify young people online or include the full names of young people in the credits of any published materials.

5.4.4 Data security

Personal data is accessed and stored securely. Access to personal data is strictly controlled.

Data is secured against loss through systems failure, theft and damage. See Mary's Data Protection Policy for further details.

6 Changes, Reviews and Approvals for this Policy

Date	Changes, Reviews and Approvals	Who By
21/07/2023	Significant changes to policy following the demerger of the organisation. • Changes to remove references to childcare specific requirements (for example Ofsted and the LA early years contacts). • Flowcharts and links updated. • Formatting and readability changes.	Aston Wood
26/07/2023	Approval	Trustees