StMARY'S

calling Islington home

# St Mary Islington

# E-Safety Guidance and Procedures

St Mary Islington
St Mary's Parish Office
Upper Street
Islington
N1 2TX
stmaryislington.org.uk

This policy should be read alongside St Mary's policies and procedures on child protection and safeguarding. More information about safeguarding and child protection can be found at

St Mary's Safeguarding Policy (see policy folder)

## The purpose of this policy statement

St Mary's works with children, young people and families as part of its activities. These include: St Mary's Youth Club for 10-19 years, St Mary's Playscheme for 6-12 years, St Mary's Pre-School for under 5s. St Mary's lets out space to many community groups of all ages.

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
- provide staff and volunteers with the overarching principles that guide our approach to online safety
- ensure that, 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 St Mary's activities.

## 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

## 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.

## 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 St 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.

## We will:

Appoint an online safety coordinator for each area of our operation.
St Mary's E-Safety leads

- Youth Club; Youth Minister, Chloe Rotter, 020 7226 3400 chloe.rotter@stmaryislington.org
- Play Scheme; Childcare Services Manager Sharon Ellis 020 7704 2873 or 07935399872 sharon.ellis@stmaryislington.org
  Pre-School; Childcare Services Manager Sharon Ellis 020 7704 2873 or 07935399872 sharon.ellis@stmaryislington.org
- Overall Operational Lead; Vicar, James Hughesdon 020 7226 3400 or 07841 123869 james@stmaryislington.org
- Trustee responsible for E-Safety; Sophie Castell, s.castell@btinternet.com 020 7226 3400

  St Mary's is committed to reviewing our policy, procedures and good practice annually The above named E-Safety leads are crucial to developing and maintaining an E-Safety culture within St Mary's.

## 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.
- St Mary's will filter all internet devices to ensure safe access for all St Mary's users. See Appendix No. 5

## 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 St Mary's Safeguarding policy

## Risks and issues

The following are the range of technologies children/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

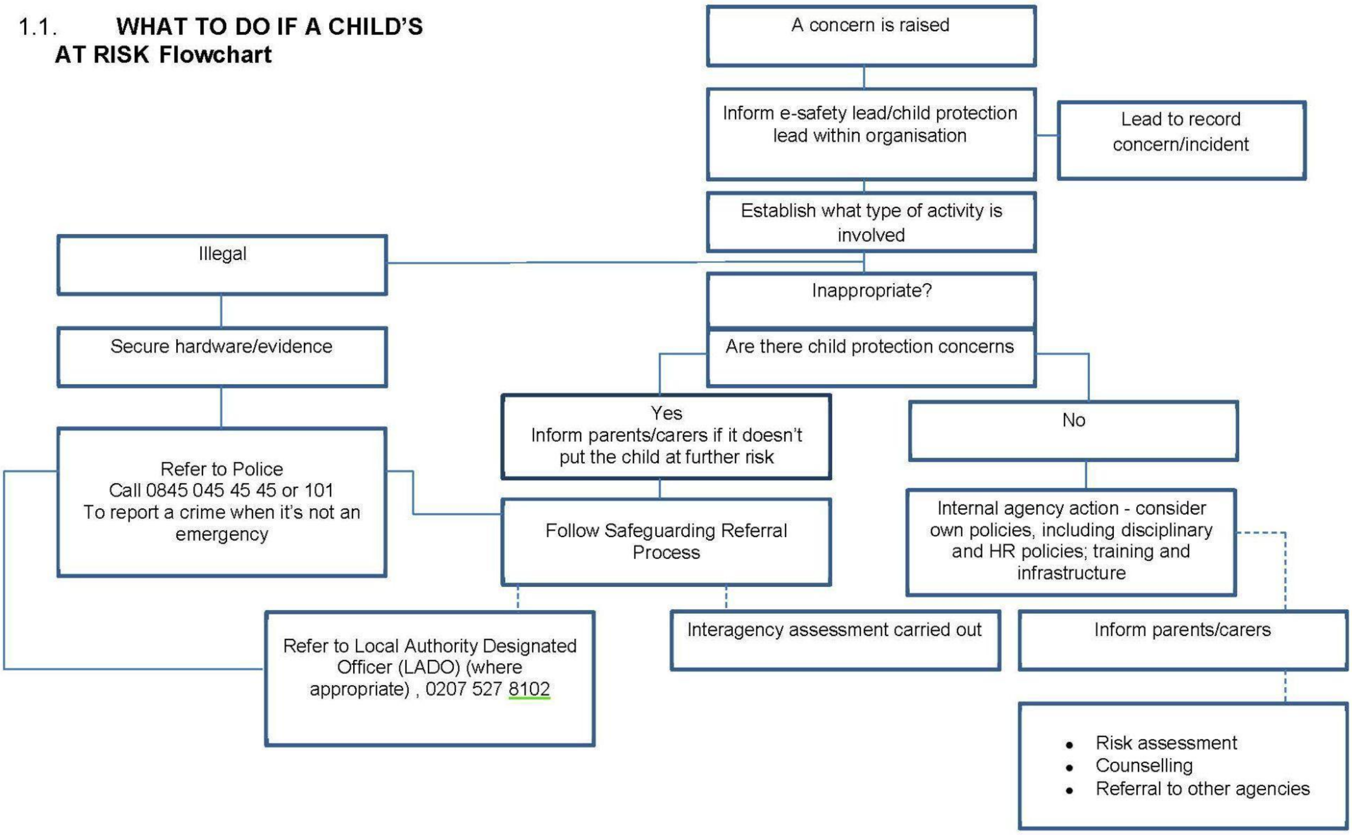
### Risks can come under the categories outlined below:

| | Commercial | Aggressive | Sexual | Values |
|---|---|---|---|---|
| **Content**<br>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**<br>Unsuitable contact from another user | Tracking Harvesting Publishing information about themselves | Being bullied, harassed, stalked | Meeting strangers Being groomed | Self-harm Unwelcome persuasions |

| | | | | |
|---|---|---|---|---|
| **Conduct**<br>User’s behaviour that creates risk either through illegal activity or lack of awareness of the potential consequences | Illegal downloading<br>Gambling<br>Hacking Financial scams | Bullying or harassing another | Creating and uploading inappropriate/ abusive material<br>‘Sexting’ | Providing misleading information/ advice |

## 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
Inappropriate?
Are there child protection concerns
Secure hardware/evidence
Yes
Inform parents/carers if it doesn't put the child at further risk
No
Refer to Police
Call 0845 045 45 45 or 101
To report a crime when it's not an emergency
Follow Safeguarding Referral Process
Internal agency action - consider own policies, including disciplinary and HR policies; training and infrastructure
Refer to Local Authority Designated Officer (LADO) (where appropriate) , 0207 527 8102
Interagency assessment carried out
Inform parents/carers
Risk assessment
Counselling
Referral to other agencies

## Related policies and procedures

This policy statement should be read alongside our organisational policies and procedures, including:

- Safeguarding and Child Protection
- Procedures for responding to concerns about a child or young person's wellbeing
- Dealing with allegations of abuse made against a child or young person
- Managing allegations against staff and volunteers
- Code of conduct for staff and volunteers
- Anti-bullying policy and procedures
- Photography and image sharing guidance
- Complaints
- Behaviour Management

## Appendix 1 E-Safety Tips for Adults working with Children and Young People

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 Facebook hijacking 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.

# Appendix 2  Acceptable Use Agreements

## CHILDREN AND YOUNG PEOPLE'S ACCEPTABLE USE AGREEMENTS

### B.1 FOR YOUNG PEOPLE OF 13 OR OVER

These rules apply to our computers, our networks (including wifi) and personal devices while on our premises. You 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 St 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 St Mary's Staff.
- Connect personal devices to St Mary's computers.
- Report any faults or issues with St 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.

## B.2 FOR CHILDREN AGED 6 TO 12

These rules apply to our computers, our networks (including wifi) and personal devices while on our premises.

- I must not look at or do anything illegal, explicit or discriminatory.
- I understand that I must not bring software, disks or memory sticks into the computer room without permission.
- I must not try and access games or software without prior permission of staff
- I must not bring in any device of my own without prior permission of parent and staff
- I must not use other people's accounts
- I must ask permission before downloading games
- The messages I send will be polite and sensible.
- I understand that I must never give out my home address or telephone number, or arrange to meet anyone.
- I must not set up accounts on site without parent and staff permission
- I will not use Internet chat rooms.
- If I see anything I am unhappy with, or I receive messages I do not like, I will tell a member of staff immediately.
- I understand that St Mary’s monitors computer usage and the Internet sites I visit.
- I understand that if I deliberately break these rules, I may not be allowed to use the Internet or the computers and parents/guardians might be informed.

These should be combined with some ‘Stay Safe’ tips

- ★ Keep your personal information safe and protect your passwords.
- ★ Remember that not everyone online is who they say they are!
- ★ Never agree to meet up with anyone you have met 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.
- ★ Always ask permission to use the internet and ask an adult which websites you can visit.
- ★ If you see anything on the internet that makes you feel uncomfortable, tell an adult that you trust.

## B.3 INTERNET ACCESS AND CONTROLS IN ST MARY’S PRE-SCHOOL

Children within the preschool will have access to the computers with the support and supervision of the pre-school staff. Access will be through a planned programme with planned sites in mind. St Mary’s staff will choose safe, fun and educational online games that children will be able to explore. These sites would be monitored for commercial content with the parental permissions in place. The use of sites such as YOUTUBE will be limited for particular interests and stories by staff for the children to view.

## Appendix 3 Parents'/Carers' Information

E-safety is concerned with safeguarding children in the early years age range in the digital world. It is about learning to understand and use new technologies and Information Communication Technology in a positive way. E-Safety is not about restricting children, but educating them about the risks as well as the benefits so they can feel confident and happy online.

To keep your children safer online:

- Know what your child is doing online much like you would offline.
- Make an effort to get computer literate; if you want to support and understand your children, you need to have a reasonable understanding of their world.
- Talk to your child. Share the experience with them and ask them to show you how they use technology.
- Be open and encourage them to talk to you.
- Establish how the internet will be used in your house.
- Agree the type of content that you would be happy for them to download, knowingly receive or send on to others.
- Discuss what will be kept private online, eg, information, bank and credit card details and photos.
- Encourage balanced use – switching off at mealtimes, bedtime.
- Use a child friendly search engine.
- Install antivirus software, filtering and firewalls.
- Secure your internet connections.
- Use parental control functions for computers, mobile phones and games consoles.
- Remember that tools are not always 100% effective and sometimes things can get past them. Locate the computer/laptop in a family room and don't allow webcams to be used unless with your consent and always in a family room under supervision.
- Encourage your child not to hesitate about coming to you about anything they see online which upsets or disturbs them.
- If your child reports a problem make sure you support them, report it or seek advice.
- Save any abusive messages or inappropriate images for evidence purposes.
- Be aware of how to report nuisance calls or texts.

## Appendix 4 Useful Contacts/Websites

**Websites**

| | |
|---|---|
| BBC Learning zone | Where to catch Educational programming for primary age |
| Child Exploitation and Online Protection Centre (CEOP) | http://ceop.police.uk/ |
| Childnet International | http://www.childnet-int.org |
| Cyberbullying | www.digizen.org |
| Cybermentors | https://cybermatters.info/ |
| Get Safe Online | http://www.getsafeonline.org/ |
| Information Commissioner's Officer | http://ico.org.uk/for_organisations/data_protection/ |
| Islington Safeguarding Children Board – E-safety page | http://www.islingtonscb.org.uk/key-practice-<br>https://aclgateway.islington.gov.uk |
| Internet Watch Foundation To report indecent content. | http://www.iwf.org.u guidance/Pages/E-safety.aspxk/ |
| *Kidsmart | http://wwwx.kidsmart.org.uk/ |
| *KnowItAll (KIA) | www.childnet-int/kia) |
| Ofsted | https://www.gov.uk/government/organisations/ofsted technologies |
| Safe network | http://www.safenetwork.org.uk/Pages/default.aspx |
| *ThinkuKnow (TUK) | www.thinkuknow.co.uk |
| UK Council for Child Internet Safety (UKCCIS) | http://www.education.gov.uk/ukccis/ |
| UK Safer Internet Centre | http://www.saferinternet.org.uk |
| 10am-4pm helpline. The professional online safety helpline can escalate a report with Facebook and other social networking sites where content needs to be removed urgently | http://www.saferinternet.org.uk/helpline<br>Tel 08443814772 |
| Vodafone have published useful guides to parents on E-Safety. | https://www.vodafone.co.uk/mobile/digital-parenting/setting-an-example<br>parenting/view_magazines.html |
| Wise Kids – promoting innovative positive and safe internet use. | www.wisekids.org.uk |
| Online Safety; A Toolkit for Early Years Settings | www.plymouth.gov.uk/early _years_toolkit.pdf |

*These websites contain activities to teach children about E-safety

## Appendix 5 Control Procedures of St Mary’s Use of ICT to Ensure Safety of Users

**Internet**

*ST MARY’S Network is protected using OpenDNS Filtering*

ADOBE Pro 11 Encryption Product to be used to send sensitive personal data which encrypts and password protects the data.

ST MARY’S's e-mail system is set up to use https protocol for added security.

**Email**

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

*The Open DNS Internet Content Filtering system provides* Trojans, malware / botnet and phishing protection. It also blocks the following content categories: gambling; Lingerie/Bikini; Sex; Tobacco; Web Spam; Adult Themes; Anime/Manga/Webcomics; Games; Hate/Discrimination; Parked Domains; Proxy Anonymisers; Tasteless; Adware; Dating; Nudity; Typo Squatting; Weapons; Pornography, phishing, alcohol, drugs, and inappropriate language.

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

**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, Play Scheme or Pre-School.

Digital images/videos of children/young people are stored in a secure location on the organisation’s network and deleted when no longer required for the permitted purpose they were taken for.

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

**Equipment**

Equipment is maintained to ensure health and safety is followed.

**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 St Mary’s Data Protection Policy for further details.