Finchley Reform Synagogue

Online Safety Policy and Procedures

Adopted: March 2021

Last Reviewed: February 2021

Next Review: March 2022

e-safety (including the use of mobile phones and cameras)

We take steps to ensure that there are effective procedures in place to protect children and vulnerable adults from the unacceptable use of Information Communication Technology (ICT) equipment or exposure to inappropriate materials whilst involved in FRS-led activities.

Procedures

- Our designated person responsible for overseeing ICT within the community is:
  Deborah Rouah-Choueke – Operations Manager
- Our designated person responsible for co-ordinating action taken to protect children and youth in the community is:
  Karen Bloom – Director of Education
- Our designated person responsible for co-ordinating action taken to protect Kindergarten children is:
  Emma Wohl – Head of Kindergarten

We are a community who value each other's privacy and treat each other with kindness and respect. We expect anybody in the synagogue building to use equipment and take photographs or recordings with these values at their heart, and to ensure they have received permission if taking photographs of others.

Information Communication Technology (ICT) equipment

- Staff and DBS-checked volunteers should only use ICT equipment belonging to the synagogue, unless agreed otherwise with Council or the Synagogue Director.
- Non-staff and volunteers may use FRS equipment under supervision of staff or a DBS-checked volunteer.

- All FRS ICT equipment is to be kept safe and fit for purpose.
- All FRS computers have virus protection installed.
- Safety settings on FRS equipment are set to ensure that inappropriate material cannot be accessed.

Internet access

- Children and vulnerable adults do not normally have access to the internet and never have unsupervised access during FRS-led activities.
- The SafeSearch portal is always used if staff access the internet with children or vulnerable adults during an FRS-led activity.
- The designated person has overall responsibility for ensuring that children and vulnerable adults are safeguarded and risk assessments in relation to online safety are completed.
- Children and vulnerable adults are taught the following stay safe principles in an age appropriate way prior to using the internet:
  - only go online at FRS when supervised during FRS-led activities
  - be kind online
  - keep information about myself safe
  - only press buttons on the internet to things I understand
  - tell a member of staff/volunteer if something makes me unhappy on the internet
- Designated persons will also seek to build children's and vulnerable adults' resilience in relation to issues they may face in the online world, and will address issues such as staying safe, having appropriate friendships, asking for help if unsure, not keeping secrets as part of social and emotional development in age appropriate ways.
- If a second-hand computer or tablet is purchased or donated to the synagogue, the designated person will ensure that no inappropriate material is stored on it before anyone uses it.
- When in use, all computers and tablets for use by children and vulnerable adults are located in areas clearly visible to others.
- Children, vulnerable adults and staff are not allowed to access social networking sites during FRS-led activities.
- Staff report any suspicious or offensive material, including material which may incite racism, bullying or discrimination to the Internet Watch Foundation at www.iwf.org.uk.

- Suspicions that an adult is attempting to make inappropriate contact with a child or vulnerable adult online are dealt with according to our Safeguarding Policy.
- The designated person ensures staff have access to age-appropriate resources to enable them to assist children and vulnerable adults to use the internet safely.
- If staff become aware that a child or a vulnerable adult is the victim of cyber-bullying, they discuss this with their parents or guardians and refer them to sources of help, such as the NSPCC on 0808 800 5000 or www.nspcc.org.uk, or Childline on 0800 1111 or www.childline.org.uk , or the National Crime Agency's Child Exploitation and Online Protection Centre at www.ceop.police.uk, and for vulnerable adults to speak to the Safeguarding Lead.

Email

Children and vulnerable adults are not permitted to access their email from FRS devices.

- Volunteers using their own devices to access their FRS email account will be DBS checked before being able to do so.
- Staff and volunteers should not access personal or work emails whilst supervising children or vulnerable adults.
- If the need arises to share personal information pertaining to children or vulnerable adults, staff and lay leaders are required to do so securely, for example password protecting any documents containing personal data, minimising the data shared and the number of people it is shared with.
- Be wary of Phishing: scammers use email or text messages to trick you into giving them your personal information. If you receive a suspicious email, including one that looks like it comes from FRS, report it to data@frs.org.uk.

Mobile phones, cameras and other recording equipment - children

- Children are encouraged not to bring mobile phones or other ICT devices with them to FRS.
- Photographs and videos of living people are personal data and therefore fall under the Data Protection Act and must be treated accordingly.
- Children are regularly reminded of their responsibility to treat each other and members of staff with due respect. This includes, but is not limited to, refraining from taking photographs of others without their permission, sharing any images on social media or each other, or accessing inappropriate material whilst on FRS property.

- If a child enters FRS for a class with a mobile phone or ICT device with them, this is stored safely either in their bag, or in a phone storage box supervised by the designated lead until the end of the session, when they can collect their device.
- The exception to this is for Friday Group, where children need their devices to access recordings for their Bnei Mitzvah learning. During Friday Group, the participants are told that their device may only be used for the purposes of the learning at hand, and their learning will always be supervised by a member of staff.

Mobile phones, cameras and other recording equipment – staff and visitors

- Personal mobile phones are only used when necessary during working hours if children or vulnerable adults are on the premises, and not in a space designated for children or vulnerable adults, which will be clearly signposted. "Please refrain from taking photos of children/people and putting them on social media. This is to maintain confidentiality as you do not have permission from other parents/individuals to use these photos publicly".
- A sign at the entrance explains that we are an accessible community and therefore there are times when events in this building are photographed and/or streamed to the internet.
- Our staff ensure that the synagogue telephone number is known to family and other people who may need to contact them in an emergency.
- If our members of staff or volunteers take their mobile phones on outings, for use in case of an emergency, they should not use them to take photographs of children or vulnerable adults. With the prior agreement of the Council or the Synagogue Director, if there is a necessity to use a personal phone to take photos of children participating in an FRS activity, the photos should be immediately uploaded to the FRS network and deleted from the device on which they were taken.
- The staff and volunteers will also avoid using their personal phone for non-essential calls while they are working.

Permission to use photographs/video

- Where parents or carers request permission to photograph or record their own children, or the vulnerable adult(s) in their care, at special events, general permission should be sought from all attendees for any participants included in the photo/video. Parents and carers are advised that they may not photograph anyone else's child or any vulnerable

adult, or upload photos of anyone else's children or vulnerable adults to social media sites, without their express permission.

- If photographs of children or vulnerable adults are used for publicity purposes, consent must be given and safeguarding risks minimised.

Social media

- Staff and volunteers are advised to manage their personal security settings to ensure that their information is only available to people they choose to share information with.
- Staff and volunteers should not accept children or vulnerable adults as 'friends' due to it being a breach of expected professional conduct.
- In the event that a member of staff or volunteer names the organisation or workplace in any social media they do so in a way that is not detrimental to the organisation or its service users.
- Staff and volunteers observe confidentiality and refrain from discussing any issues relating to their role at FRS on social media
- Staff and volunteers should not share information they would not want children, parents, vulnerable adults or their carers, or colleagues to view on their personal social media accounts.
- Staff and volunteers should report any concerns or breaches to the Designated Safeguarding Lead
- Staff and volunteers will undertake regular safeguarding updates from their Designated Safeguarding Lead, to ensure they are up to date with all policies and procedures
- Staff and volunteers will declare any conflict of interest relating to relationships within the community which could have a negative impact on their role. This declaration is shared with the Designated Safeguarding Lead for their area of FRS work and updated annually.

Use and/or distribution of inappropriate images

- Staff and volunteers are aware that it is an offence to distribute indecent images.
- In the event of a concern surrounding the sharing of indecent images, the Safeguarding Children and Child Protection policy in relation to allegations against staff and/or responding to suspicions of abuse is followed.

- Staff and volunteers are aware that grooming children and young people online is an offence in its own right and concerns about a colleague's or others' behaviour in this regard are reported (as above).

Further guidance

- NSPCC and CEOP *Keeping Children Safe Online* training: www.nspcc.org.uk/what-you-can-do/get-expert-training/keeping-children-safe-online-course/

This policy was adopted by	FRS	*(name of provider)*
On	1st March 2021	*(date)*
Date to be reviewed	March 2022	*(date)*
Signed on behalf of the provider		
Name of signatory	Deborah Rouah-Choueke	
Role of signatory (e.g. chair, director or owner)	Operations Manager	