Maidenhead Synagogue E-Safety Policy

This policy relates to all members of the community who have access to, and are users of ICT systems and resources both in and out of learning venues where actions relate to religion school lessons or/and youth activities.

Context:

The aim of Maidenhead synagogue religion school is to instil a love of Judaism in the children first and foremost; this goal should stimulate their curiosity, which in turn will drive them to do some self research using a variety of technologies. However, technologies present risks to vulnerable groups as well as benefits.

 Internet use for lessons, home, social and leisure activities is expanding across all sectors of society. This brings children as well as teachers, assistants and volunteers into contact with a wide variety of influences some of which may be unsuitable.

These new technologies are enhancing communication and the sharing of information, which inevitably challenge the definitions and boundaries of the synagogue environment. Current and emerging technologies include:

Internet websites

Instant messaging

Social networking sites

Emails

Blogs

Podcasting

Video broadcasting sites

Chat rooms

Gaming and gambling sites

Music download sites

Mobile phones with camera and video functionality

Digital cameras

Smart phones, tablets and computers with e-mail and web applications

All of these have potential to help raise standards of learning, but may equally present challenges to both learners and tutors in terms of keeping themselves safe.

These challenges include:

Exposure to inappropriate material Cyber-bullying via websites, social media, mobile phones or other technologies

Identity theft or invasion of privacy

Downloading copyrighted materials

Exposure to inappropriate advertising online gambling and financial scams

Safeguarding issues such as grooming

Other illegal activities

As we seek to maximise the educational benefit that can be obtained by exploiting the use of ICT, we have to minimise any associated risks. By making clear to learners, staff and other members of the synagogue what expectations are regarding the use of ICT, we aim to protect both children and teachers and other helpers from harm, as far as reasonably practicable. The precise nature of the risks faced by users will change over time as technologies, fads and fashions change but there are general principles of behaviour and the code of conduct that apply to all situations e.g.:

• all users need to know what to do if they come across inappropriate material,

• adult stakeholders should not give out their personal information to learners such as their personal telephone numbers or email address,

• adult stakeholders should not allow access to their personal social networking site accounts.

We must also communicate to the children that they should not give out their personal information such as telephone numbers; addresses etc. to strangers or publish this information on social networking sites.

A balance needs to be struck between educating staff and pupils to take a reasonable approach towards the use of regulation and technical solutions. We must recognise that there are no totally effective solutions to moderate and control the internet, so this policy incorporates both approaches.

Roles and Responsibilities

1) Teachers, teaching assistant and activity leaders

All staff and volunteers (as well as suppliers and contractors) are responsible for supporting the safe behaviour and following e-safety procedures. They should all be familiar with the E-safety and Acceptable use of ICT policy (AUP) as well as their relevance to the code of conduct and safeguarding policies.

All staff should:

• participate in any e-safety training and awareness raising sessions

• Act in accordance with the AUP and e-safety policy

• report any suspicion of misuse to the designated persons or a Council member

• avoid making any comment regarding Maidenhead synagogue, its community or judaism in general that could be construed as negative on any blogs or social network sites.

• help educate learners in keeping safe especially with vulnerable groups.

Whilst regulation and technical solutions (such as filtering systems) are important,

they must be balanced with educating learners to take a responsible approach. The

education of learners in e-safety is an essential part of using technology in classes.

• act as a good role model in their own use of ICT.

• be aware of the potential for cyber-bullying in their sessions where

malicious messages e.g. through the use of forums and social networking sites, or

via internal class emails or text messages on mobile phones etc, which can cause

hurt or distress.

It should also be noted:

• where Internet use is pre-planned in sessions or enrichment activities, learners

should be directed to sites which are appropriate for their use and procedures should

be followed for reporting any unsuitable material that is found on Internet searches

(where practicable, pre-check sites and any possible searches should be pre-checked).

• where learners are able to freely search the Internet, staff should be vigilant in monitoring the content of websites in case there is any unsuitable material.

 • children should be taught to be critically aware of the materials/content they can access online and be guided to validate the accuracy of information.

• wherever possible the children should be educated of the need to acknowledge the sources of any information used and to respect copyright when using material accessed on the Internet.

Important: to avoid divulging email addresses by mistake, use the BCC address label when sending emails to groups to prevent circulation of emails.

2) Learners

The provision of ICT resources and facilities are a privilege, not a right. Learners are encouraged to access various technologies in lessons and in the completion of assignments and independent research,and are therefore expected to follow the synagogue's AUP. They should fully participate in e-safety activities

and report any suspected misuse to a member of staff. Learners are required to follow the guidelines of our e-safety policy which are summarized in the code of conduct.

Learners are expected to:

• behave in a safe and responsible manner;

• treat equipment with respect;

• use USB/Flash memory key(s) only for educational purposes;

• be polite and not use email, social media or blogs etc to make negative comments, bully or insult others;

• use the resources only for educational purposes;

• not reveal their passwords;

• not use chat rooms or newsgroups.

3) Synagogue Council:

Every member takes e-safety very seriously and will ensure that policies and procedures are in line with best practice and the safeguarding agenda. In particular they will ensure that all staff receive suitable training and development to carry out their e-safety roles and sufficient resources are allocated to the task. The Chairman, the Safeguarding and Child Protection Coordinator, the Designated Safeguarding Lead will follow the correct procedure in the event of a serious e-safety allegation being made against a member of staff and ensure that there is a robust system in place for monitoring e-safety. This includes making sure that the academic network infrastructure is safe and secure and that policies and procedures approved within this policy are implemented. Regular review of the issues will take place at the safeguarding working group meetings with feedback sessions scheduled to the senior management team meetings.

Responding to issues

It is important that any incidents are dealt with as soon as possible in a proportionate manner and that members of the community are aware those incidents have been dealt with. Any concerns around the misuse of ICT must follow the referral process within the safeguarding policy and procedure where there is a potential threat to another learner, vulnerable person or member of staff. Any suspected misuse must be reported to the Designated Safeguarding Lead to agree an appropriate course of actions.

Where it is suspected that any misuse might have taken place and dependent on the nature of misuse, the disciplinary procedure will be invoked. Where an allegation has been made against a student an investigation will take place by the Principal or the Designated Safeguarding Lead. The outcome of the investigation will decide what the appropriate course of action will be and depending on the nature of the misuse the student could be suspended from classes till the investigation is complete. The student code of conduct procedure will be invoked should the allegation be found to be true and the sanction will depend on the seriousness of the misuse and whether it was accidental or deliberate, a first time offence,

thoughtless or malicious e.g.: intended to cause harm to others. Sanctions could involve the person concerned having ICT access removed for a period of time or in very serious cases, exclusion. Where there is a potential legal issue the Chair of the Council will decide on the need for involvement of outside agencies including the police, together with the designated persons in line with our safeguarding and other policies.