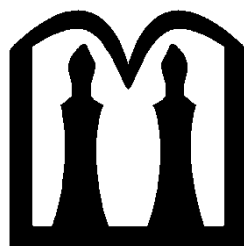


BEIS YAAKOV JEWISH HIGH SCHOOL ACADEMY



בית ספר לבנות בית יעקב

E- SAFETY POLICY

Date of Approval 2nd March 2015

Date of Next Review: Spring 2016

Term of Review Annually

Committee: C & R

Prepared By: CB

Signed:

(Chairman)

Changes Made	Date

E- Safety

IT Manager: Mr V Schwinger

Head of ICT: Mrs A Singer

e-safety officer: Mrs Thursch

Rationale for creating a school e-safety policy

Whilst the internet and associated technologies are an excellent tool and resource to enrich learning there are still dangers related to their use, especially in relation to young students.

As a school it is our duty of care alongside that of parents and other members of the community to safeguard our children from these dangers and this can be achieved by many different mechanisms working together.

The Ethos of Beis Yaakov Jewish High School Academy is governed by the codes of Torah observance. The School expects its pupils to have no access to any inappropriate media which means that parents have to ensure that their children do not have access to the internet or any other media not meeting the stringent moral criteria of the Charedi community.

The school support parents in understanding the issues and risks associated with children's use of digital technologies. The schools take an active role in providing information and guidance for parents on promoting e-safety messages.

This policy will be reviewed annually by SLT and governors or more frequently in response to new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Identification of Risks

The use of these new technologies can put young people at risk within and outside the school. Some of the dangers they may include:

- Access to illegal, harmful or inappropriate images or other content
- Unauthorised access to / loss of / sharing of personal information
- The risk of being subject to grooming by those with whom they make contact on the internet.
- The sharing / distribution of personal images without an individual's consent or knowledge

- Inappropriate communication / contact with others, including strangers
- Cyber-bullying via email & SMS chats, and other social media and chatrooms
- Access to unsuitable video / internet games
- An inability to evaluate the quality, accuracy and relevance of information on the internet
- Plagiarism and copyright infringement
- Illegal downloading of music or video files
- The potential for excessive use which may impact on the social and emotional development and learning of the young person
- digital footprints , cyber- crime and hackers/virus (of all types)
- web-camera's on computer

Many of these risks reflect situations in the off-line world and it is essential that this e-safety policy is used in conjunction with other school policies (e.g. safeguarding, behaviour, anti-bullying and Child protection policies)

The e-safety policy that follows explains how the school intends to provide the necessary safeguards to help ensure that it has done everything that could reasonably be expected to manage and reduce these risks, while also addressing wider educational issues in order to help parents / carers to be responsible users and keep their children stay safe while they are using the internet and other communications technologies.

General Policy statement

The academy will endeavour to ensure the e-safety of all academy members

Education – Students

- Participating in and gaining an understanding of e-safety issues and safe responses from e-safety training sessions
- A planned e-safety programme will be provided as part of ICT lessons and supported in kodesh subjects
- Key e-safety messages will be reinforced as part of a planned programme of extra-curricular education for example external institutions.
- Students will be taught as appropriate to their age and maturity to be critically aware of the materials / content that is downloaded from the internet and guided to validate the accuracy of information.

Education – Parents / Carers

As parents / carers play an essential role in the education of their children and in the monitoring /regulation of the children's on-line experiences.

In order support parents/ careers understanding of e-safety risks and issues we will

- Prepare a leaflet explaining the design and use of the internet. Additionally point out potential danger encountered when using the internet
- Annual Parents awareness evenings (minute and recording are available for parents unable to attend)

Education & Training – Staff

It is essential that all staff receive e-safety training and understand their responsibilities, as outlined in this policy. Training will be offered as follows:

- This E-Safety policy and its updates will be presented to and discussed by staff in SLT/SMT and general staff meetings as appropriate.
- Staff are expected to be vigilant to only download and show students materials that meet the standards of the ethos of the school.
- Staff are responsible to ensure students do not use their computers without adult supervision
- Staff are responsible to log off their classroom computers upon exiting

Network Safety

- IT Manager ensure the internet has filters so only appropriate material can be accessed
- Controls have been put in place by the IT Manager so no pupil can access the internet on their username
- USB ports are locked for student use in order to control the contents saved onto the intranet.
- The e-safety officer regularly monitors the intranet to ensure appropriateness.

Infringements of e-safety policy are dealt with initially by the SMT and depending on the severity of the infringement they are referred onto the SLT through the pastoral system.