Yesoiday HaTorah Multi Academy Trust

E-Safety Policy

Approved February 2016
Updated January 2023
Next review January 2024

Introduction

The staff and governors at Yesoiday HaTorah Multi Academy Trust recognise the benefits and opportunities which new and existing technologies offer teaching and learning. We run the school according to our orthodox Jewish ethos and synchronise all educational decisions and choices with this ethos. We are very careful to provide the children with opportunities to learn and enhance skills using technology in order to promote achievement and enable lifelong learning. However, the accessibility and global nature of the internet and different technologies available mean that we are also aware of potential risks and challenges associated with such use. Our approach is to implement appropriate safeguards and vetting procedures within the school while supporting staff and learners. We believe this can be achieved through a combination of security measures, training, guidance and implementation of our policies. In furtherance of our duty to safeguard learners and the Every Child Matters agenda, we will do all that we can to make our learners and staff stay e-safe and to satisfy our wider duty of care. This e-safety policy should be read alongside other relevant school policies [e.g. Safeguarding, Acceptable Use, e-Security, Anti Bullying, Disciplinary and Child Protection.]

Monitoring and Reviewing

Yesoiday HaTorah Multi Academy Trust's e-Safety team is made up of the e-Safety Officer, Ethos Manager (Rebbe Yodaiken) the Designated Safeguarding Lead (Mrs Young/Mrs Greenberg/Mrs Itzinger/Rabbi Harris), , a Governor and the IT Coordinator (Mrs Rosenhead/Rebbe Green). Consultation is carried out before the policy is approved at each review date. The next review date is January 2024 or with any significant change.

The committee will also monitor the impact of the policy at that time. The policy will also be reconsidered where particular concerns are raised or where an e-safety incident has been recorded.

Policy Scope

The policy applies to all users and learners and staff/all members of the school community who have access to the IT systems, both on the premises and remotely. Any user of the school IT systems must adhere to this e-Safety Policy and the Acceptable Use Agreement (available from the office or see appendices). The e-Safety Policy applies to all use of the internet and forms of electronic communication such as email, mobile phones and social media sites.

Roles and Responsibilities

There are clear lines of responsibility for e-safety within the school. The first point of contact should be the Designated Safeguarding Lead. All staff are responsible for ensuring the safety of learners and should report any concerns immediately to their line manager. All teaching staff are required to deliver e-safety lessons (in line with our ethos and the curriculum set out in our program of study) to classes and to read through and adhere to the incident reporting procedure as contained in the appendices. When informed about an e-safety incident, staff members must take particular care not to guarantee any measure of confidentiality towards either the individual reporting it, or to those involved.

All learners must know what to do if they have e-safety concerns and who to talk to. In most cases, this will be Mrs Young or Rebbe Yodaiken. Where any report of an e-safety incident is made, all parties should know what procedure is triggered and how this will be followed up. Where management considers it appropriate, the Designated Safeguarding Lead may be asked to intervene with appropriate additional support from external agencies.

E-Safety Officer Responsibilities:

The e-Safety Officer, in conjunction with the Computing Coordinator, is responsible for keeping up to date with new technologies and their use, as well as attending relevant training. They will be expected to lead the e-Safety Group, complete, review and update the e-Safety Policy, deliver staff development and training, record incidents, report any developments and incidents to the relevant parties or authorities and liaise external agencies to promote e-safety within the school community. They may also be required to facilitate workshops for parents.

Learner Responsibilities:

Learners are responsible for using the school IT systems in accordance with the school e-Safety Rules. Learners must act safely and responsibly at all times when using the computers and other items of technology. They are responsible for attending e-safety lessons as part of the curriculum. They must follow reporting procedures where they are

worried or concerned, or where they believe an e-safety incident has taken place involving them or another member of the school community.

Staff Responsibilities:

All staff are responsible for using school IT systems and mobile devices in accordance with the school [staff] Acceptable Use Policy [see appendices] and this policy, which they must read. Staff are responsible for attending staff training on e-safety and displaying a model example to learners at all times through embedded good practice.

There should be no digital communications with learners outside of school. Online communication with learners is restricted to the school network or Learning Platforms such as Purple Mash. External platforms not hosted by the school, such as social media sites, may never be used neither in nor out of school with the specific exception of Trello.com.

This policy will, be monitored and kept under review.

All staff should apply relevant school policies and understand the incident reporting procedures. Any incident that is reported to or discovered by a staff member must be reported to the e-Safety Officer and/or line manager without delay. Further information is available from the e-safety officer, DSL or ethos manager.

Security – Cyber Prevention Plan

The school will do all that it can to make sure the school network is safe and secure. Every effort will be made to keep security software up to date. Appropriate security measures will include the use of enhanced filtering, antivirus software and protection of firewalls, servers, routers, work stations etc. to prevent accidental or malicious access of school systems and information. Relevant protection will also be applied to digital communications, including email, over the school network.

All USBs used in school are required to be encrypted and protected by a password. This is available through the school by contacting the IT coordinator.

Staff will receive cyber security training and the Trust has registered with the Police Cyber Alarm scheme.

Risk Assessment

When wishing to introduce new technologies and or websites, staff must first carry out a risk assessment for e-safety and ethos issues, (see appendices). A risk assessment must also

be carried out where a learner is learning off site. All forms must be submitted to the e-Safety Officer and Ethos Manager for their consideration and approval.

Behaviour

Yesoiday HaTorah Multi Academy Trust will ensure that all users of technologies adhere to the standard of behaviour as set out in the Acceptable Use Policy.

The school will not tolerate any abuse of IT systems. Whether offline or online, communications by staff and learners should be courteous and respectful at all times. Any reported incident of bullying or harassment or other unacceptable conduct will be treated seriously and in line with the student and staff disciplinary codes.

Where conduct is found to be unacceptable or illegal, current procedure will be followed, either dealing with issues internally or, where directed by the head teacher, outside agencies (LA, social services, police) will be brought in [see appendix for full procedure].

Communications

Yesoiday HaTorah Multi Academy Trust requires all users of IT to adhere to the acceptable use policies relevant to them, i.e. learners, staff, parents or governors.

Use of Images and Video

The use of images, or photographs, is popular in teaching and learning and should be encouraged where there is no breach of copyright or other rights of another person (e.g. images rights or rights associated with personal data). This will include images downloaded from the internet and those belonging to staff or learners.

The use of personal mobile phones to take digital images of children is not permitted. The use of personal cameras, mobile phone cameras or other recording equipment is prohibited in school at all times.

All staff should receive training on the risks when taking, downloading and posting images online and making them available to others, whether in or out of school. There are particular risks where personal images of themselves or others are posted onto social networking sites, for example.

All learners should receive training on the risks when taking, downloading and sharing images.

Yesoiday HaTorah teaching staff will provide information to learners on the appropriate use of images as detailed in the Photography policy. This includes photographs of learners and staff as well as using third party images. Our aim is to reinforce good practice as well as offer further information for all users on how to keep their personal information safe.

No image/photograph can be copied, downloaded, shared or distributed online without permission from the SLT or head teacher. Photographs of activities on the school premises should be considered carefully and have the consent of the SLT and (parents where relevant) before being published. Approved photographs should not include names of individuals without consent. This excludes Trello.com for the purpose of providing evidence of achievement.

Remote Learning

Staff are expected to follow school guidelines in the event of remote learning. This may change from time to time and staff should ensure they have the most up to date guidelines from their manager. Zoom / Skype / Telephone conferencing and other such systems should only be used if instructed and must comply with all guidance issued.

Trello.com

The school will use the social networking site Trello.com to store, share, monitor, and record events and evidence of learners' achievements, progress, participation in school schemes and events. It will further be used for tracking and storing policies, minutes of meetings and other items that the SLT and management feel it will help organise and store. This will include pictures of teachers and pupils and/or their work. This website has been checked and is secure, has its own GDPR policy and AUP that the school has read and fits in with our own. Only people designated by the Head Teacher, Deputy Head Teacher or SLT will be invited to access any boards and the decision will be based on need and role.

Although Trello.com can be accessed on any internet enabled device, the pictures and information are stored on the website and therefore accessing this at home or on a personal device does not contradict the mobile phone use policy or the Photography Policy.

Personal Information

Personal information is information about a particular living person. Yesoiday HaTorah Multi Academy Trust collects and stores the personal information of learners and staff regularly e.g. names, dates of birth, email addresses, assessed materials and so on. The school will keep that information safe and secure and will not pass it onto anyone else without the express permission of the parents or staff.

No personal information can be posted to the school website without the permission of the governors and only if it is in line with our Data Protection Policy [see appendices]. Only names of the governors will appear on the school website and neither staff nor learners' personal information will be available on the website.

Staff must keep learners' personal information safe and secure at all times. When using an online platform, for example Purple Mash, all personal information must be password protected. No personal information of individuals is permitted offsite unless the member of staff has the permission of the Designated Safeguarding Lead or the head teacher. Every user of IT facilities is required to log off or lock the device on completion of any activity, or where they are physically absent from a device for any period.

No school mobile device such as a laptop, are allowed of premises without consent from the head teacher and IT Coordinator.

Where the personal data is no longer required, it must be securely deleted in line with the Data Protection Policy.

Education and Training

With the current unlimited nature of internet access, it is impossible for the school to eliminate all risks for staff and learners. It is our view therefore, that the school should support staff and learners to stay e-safe through regular training and education. This will provide individuals with skills to be able to identify risks independently and manage them effectively.

For learners:

Learners will attend e-safety lessons in accordance with the school Computing Scheme of Work and school ethos.

Issues associated with e-safety apply across the curriculum and learners should receive guidance on what precautions and safeguards are appropriate when making use of the technologies. Learners should also know what to do and who to talk to where they have concerns about inappropriate content, either where that material is directed to them, or where it is discovered as part of a random search.

Within classes, learners will be encouraged to question the validity and reliability of materials researched, viewed or downloaded. They will also be encouraged to respect the copyright of other parties and to cite references properly.

For staff:

Staff will take part in mandatory e-safety training each school year. This will be led by the e-Safety Officer and IT Coordinator. Further resources of useful guidance and information will be issued to all staff following the session.

Any new or temporary users will receive training on the school IT system, led by the Computing Coordinator.

For governors:

Training for governors will be provided on a frequency relevant to our needs.

For parents:

Training for parents will be offered on a frequency relevant to our needs and the needs of our community.

Incidents and Response

Where an e-safety incident is reported to the school this matter will be dealt with very seriously. The school will act immediately to prevent, as far as reasonably possible, any harm or further harm occurring. If a learner wishes to report an incident, they can do so to their class teacher or to the school e-Safety Officer or any member of the SLT or the head teacher. Where a member of staff wishes to report an incident, they must contact their line manager as soon as possible. Following any incident, the school will review what has happened and decide on the most appropriate and proportionate course of action. Sanctions may be put in place, external agencies may be involved or the matter may be resolved internally depending on the seriousness of the incident. The flow chart in the appendices lists behaviours and their consequences. This is in line with the school Acceptable Use Policy. Serious incidents will be dealt with by senior management, in consultation with appropriate external agencies.

Feedback and Further Information

Yesoiday HaTorah Multi Academy Trust welcomes all constructive feedback on this and any other school policy. If you would like further information on e-safety, or wish to make any comments on our e-Safety Policy, then please contact, our e-Safety Officer or Head teacher via the school office.

This policy has been drafted using information and resources provided by JISC Legal Information.

Relevant Policies

- Safeguarding
- Anti-Bullying
- Disciplinary
- Child Protection
- Photography Policy
- Data Protection Policy
- Cyber Prevention Plan

Appendices

- Acceptable Use Policy
- Incident Reporting Procedure
- Risk Assessment
- Cyber Security Training For School Staff

YHMAT Staff Acceptable Use Policy

As a professional organisation with responsibility for children's safeguarding it is important that all staff take all possible and necessary measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft. All members of staff have a responsibility to use the school's computer system in a professional, lawful, and ethical manner. To ensure that members of staff are fully aware of their professional responsibilities when using Information Communication Technology and the school systems, they are asked to read and sign this Acceptable Use Policy.

This is not an exhaustive list and all members of staff are reminded that ICT use should be consistent with the school ethos, other appropriate school policies, relevant national and local guidance and expectations, and the Law.

1. I understand that Information Systems and ICT include networks, data and data storage, online and offline communication technologies and access devices. Examples include laptops, mobile phones, tablets, digital cameras, email and social media sites**.**

2. School owned information systems must be used appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

3. I understand that any hardware and software provided by my workplace for staff use can only be used by members of staff and only for educational use. To prevent unauthorised access to systems or personal data, I will not leave any information system unattended without first logging out or locking my login as appropriate.

4. I will respect system security and I will not disclose any password or security information and will use a 'strong' password (A strong password has numbers, letters and symbols, with 8 or more characters, does not contain a dictionary word and is only used on one system and is changed regularly).

5. I will not attempt to install any purchased or downloaded software, including browser toolbars, or hardware without permission from the system manager.

6. I will ensure that any personal data of pupils, staff or parents/carers is kept in accordance with the Data Protection Act 1998. This means that all personal data will be obtained and processed fairly and lawfully, only kept for specific purposes, held no longer than necessary and will be kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely (e.g. via VPN). Any data which is being removed from the school site (such as via email or on memory sticks or CDs) will be protected in a method approved by the school. Any images or videos of pupils will only be taken and used as stated in the school image use policy (photography policy available from the school office) and will always take into account parental consent.

7. I will not keep or access professional documents which contain school-related sensitive or personal information (including images, files, videos, emails etc.) on any personal devices (such as laptops, digital cameras, mobile phones), unless they are suitably secured and encrypted. I will protect the devices in my care from unapproved access or theft.

8. I will not store any personal information on the school computer system including any school laptop or similar device issued to members of staff that is unrelated to school activities, such as personal photographs, files or financial information.

9. I will respect copyright and intellectual property rights.

10. I have read and understood the school e-Safety policy which covers the requirements for safe ICT use, including using appropriate devices, safe use of social media websites and the supervision of pupils within the classroom and other working spaces (e-safety policy available from the school office).

11. I will report all incidents of concern regarding children's online safety to the Designated Safeguarding Lead (Mrs Young/Mrs Itsinger/Rabbi Harris) and/or the e-Safety Coordinator as soon as possible. I will report any accidental access, receipt of inappropriate materials, filtering breaches or unsuitable websites to the Designated Safeguarding Lead and/or the e-Safety Coordinator and/or the Ethos Manager (Rebbe Menachem Yodaiken) as soon as possible.

12. I will not attempt to bypass any filtering and/or security systems put in place by the school. If I suspect a computer or system has been damaged or affected by a virus or other malware, or if I have lost any school related documents or files, then I will report this to the Computing Coordinator (Mrs Rosenhead/Rebbe Green) as soon as possible.

13. My electronic communications with pupils, parents/carers and other professionals will only take place within clear and explicit professional boundaries and will be transparent and open to scrutiny at all times. All communication will take place via school approved communication channels e.g. via a school provided email address or telephone number and not via personal devices or communication channels e.g. personal email, social networking or mobile phones. Any pre-existing relationships or situations that may compromise this will be discussed with the Senior Leadership team and/or Head Teacher.

14. I will ensure that my online reputation and use of ICT and information systems are compatible with my professional role, whether using school or personal systems. This includes the use of email, text, social media/networking, gaming and any other devices or websites. I will take appropriate steps to protect myself online and will ensure that my use of ICT and internet will not undermine my professional role, interfere with my work duties and will be in accordance with the school AUP and the Law.

15. I will not create, transmit, display, publish or forward any material that is likely to harass, cause offence, inconvenience or needless anxiety to any other person, or anything which could bring my professional role, the school, or the County Council, into disrepute.

16. I will promote online safety with the pupils in my care and will help them to develop a responsible attitude to safety online, system use and to the content they access or create, within the school ethos.

17. If I have any queries or questions regarding safe and professional practise online either in school or off site, then I will raise them with the Designated Safeguarding Lead and/or the e-Safety Coordinator or the Head Teacher.

18. I understand that my use of the information systems, Internet and email may be monitored and recorded to ensure policy compliance.

The School may exercise its right to monitor the use of information systems, including Internet access and the interception of e-mails in order to monitor compliance with this Acceptable Use Policy and the School's Data Security Policy. Where it believes unauthorised and/or inappropriate use of the service's information system or unacceptable or inappropriate behaviour may be taking place, the School will invoke its disciplinary procedure. If the School suspects that the system may be being used for criminal purposes or for storing unlawful text, imagery or sound, the matter will be brought to the attention of the relevant law enforcement organisation.

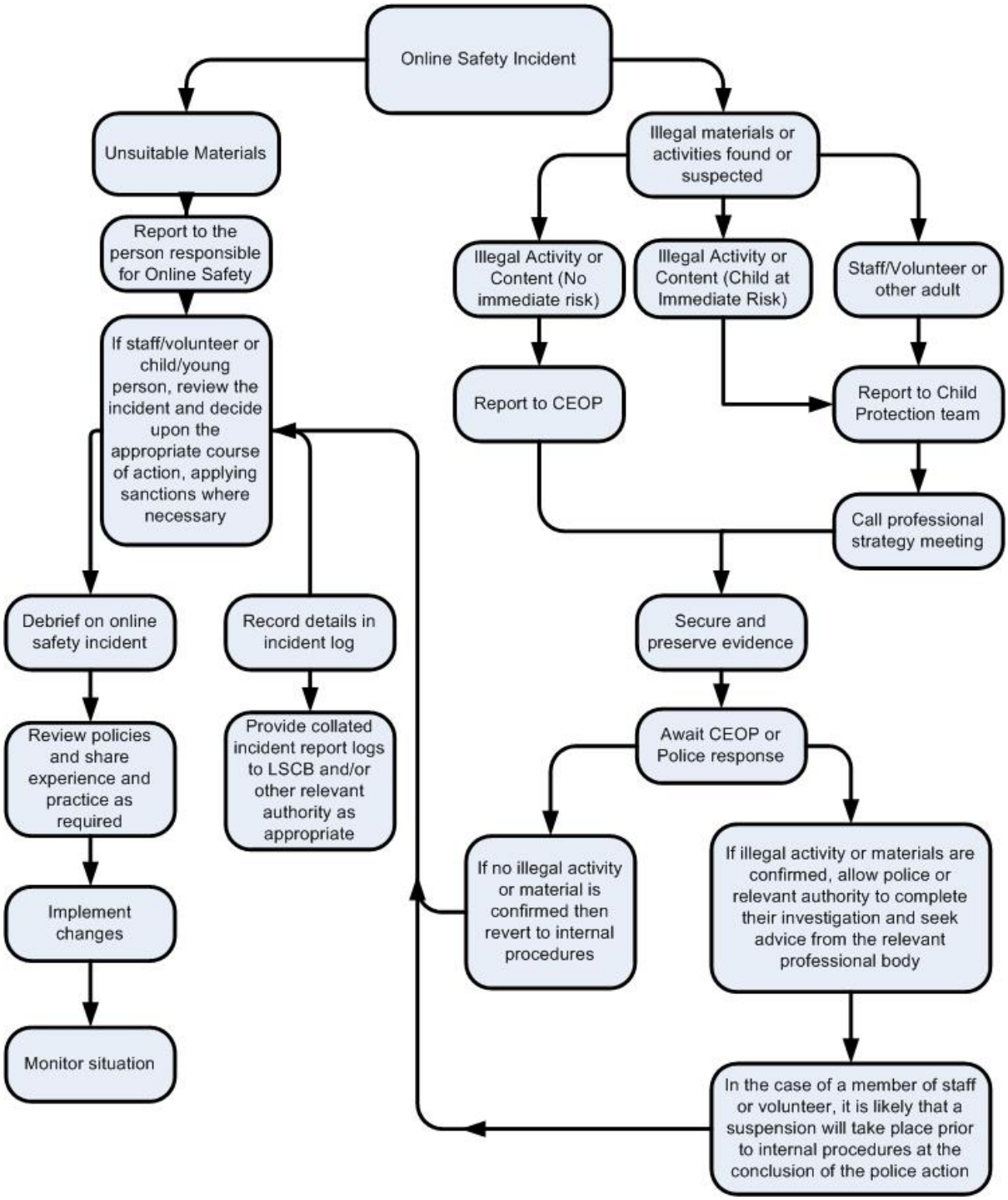
I have read and understood and agree to comply with the Staff Acceptable Use Policy.

Signed: ……... Print Name: …… Date: ……

Accepted by: …… Print Name: ……..

Appendix 2 – Incident Reporting Procedure

Responding to incidents of misuse – flow chart



Record of reviewing devices / internet sites (responding to incidents of misuse)

Group	
Date	
Reason for investigation	

Details of first reviewing person

Name	
Position	
Signature	

Details of second reviewing person

Name	
Position	
Signature	

Name and location of computer used for review (for web sites)

Web site(s) address / device Reason for concern

Conclusion and Action proposed or taken

(Created from **SWGfL E-Safety School Template Policies)**

E-Safety Risk Assessment

Name of individual:

Staff completing Risk Assessment:
Date:

Activity / Program / Website	**Educational Value**	**Risks Identified**	**Precautions that will be taken**	**Authorisation** *(by e-safety officer Mr Spielman and ICT Coordinator, Rebbe Green)*

Activity / Program / Website	Educational Value	Risks Identified	Precautions that will be taken	**Authorisation** *(by e-safety officer Mr Spielman and ICT Coordinator, Rebbe Green)*

Additional comments

Risk assessment shared with:

Next review date: