HASMONEAN MULTI-ACADEMY TRUST

HASMONEAN

אל תקרי בניך אלא בוניך

E-Safety and the Acceptable Use of The Internet and Trust Network Policy

Note: All Internet and email activity is subject to monitoring

E-Safety Officer – Boys' School	Ms R Benarroch	r.benarroch@hasmonean.co.uk
E-Safety Officer – Girls' School	Mrs L Waugh	l.waugh@hasmonean.co.uk
E-Safety Governor	TBC	
Network Manager	Mr O Smirnov	o.smirnov@hasmonean.co.uk

Introduction

The Internet has the potential to be a valuable educational resource, benefiting students, parents and teachers. All students and staff should have access to the Internet and the Trust's ICT Network within clearly specified guidelines. Staff and students at the Trust will be encouraged to make use of ICT in their work and, where necessary, training will be provided. An important part of the training will be guidance on how to evaluate web pages and where to find suitable sites. All members of the school community wishing to use the Trusts Network will be required to read this policy.

However, the use of these new technologies can put young people at risk within and outside of the Trust. Some of the dangers they may face include:

- Access to illegal, harmful or inappropriate images or other content;
- Unauthorised access to, loss of or 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 or contact with others, including strangers;
- Cyber-bullying including racist, sexual, homophobic, biphobic and transphobic comments;
- Access to unsuitable video and 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.

Many of these risks reflect situations in the off-line world and it is essential that this policy is used in conjunction with other school policies, including the Behaviour Policy, Safeguarding Policy, Mobile Phone Policy and Data Protection Policies.

It is impossible to eliminate these risks completely. It is therefore essential, through good educational provision, to build students' resilience to the risks which they may be exposed to, so that they have the confidence and skills to face and deal with these risks.

The Trust has provided the necessary safeguarding provisions for students to help ensure that the Trust has done everything that could reasonably be expected of them to manage and reduce these risks. Safeguarding is a serious matter and we use technology and the Internet extensively across all areas of the curriculum. Online safeguarding, known as e-safety is an area that is constantly evolving and, as such, this policy will be reviewed on an annual basis or in response to an e-safety incident, whichever is sooner. This policy explains how we ensure safeguarding provisions are in place, while also addressing wider educational issues in order to help young people and their parents to be responsible users and stay safe while using the internet and other communication technologies for educational, personal and recreational use.

As part of the staff induction process, all new staff will receive information and guidance on the schools acceptable use policies, and the reporting procedures.

Roles and Responsibilities for the CEO, Executive Leadership team (ELT) and Senior Leadership Team (SLT):

- The CEO is responsible for ensuring the safety (including e-safety) of members of the Trust community, though responsibility for the oversight of e-safety will be delegated to the relevant staff who are likely to include the E-Safety Officer, Designated Safeguarding Lead; ELT Line Manager for Computing; SLT Line Manager for Computing; Subject Leader for Computing and the Network Manager, as appropriate;
- The CEO, ELT and SLT are responsible for ensuring that the E-Safety Officer and other relevant staff receive suitable Continuing Professional Development (CPD) to enable them to carry out their e-safety roles and to train other colleagues, as relevant;
- The CEO, ELT and SLT will ensure that there is a system in place to allow for monitoring and support of those in school who carry out the internal e-safety monitoring role. This is to provide a safety net and also support those colleagues who take on important monitoring roles;
- The ELT, SLT and the Designated Safeguarding Lead should be aware of the procedures to be followed in the event of a serious e-safety allegation being made against a member of staff.

Appoint one governor to have overall responsibility for the governance of e-safety at
the Trust who will:

- Keep up to date with emerging risks and threats through technology use.
- Receive regular updates from the CEO and Headteacher in regards to training, identified risks and any incidents.

Roles and Responsibilities for the E-Safety Officer:

- leads the e-Safety committee;
- takes day to day responsibility for the oversight of e-safety issues and has a leading role in establishing and reviewing the Trust's e-safety policies and documents;
- ensures that all staff are aware of the procedures that need to be followed in the event of an e-safety incident taking place;
- liaises with the Local Authority, where relevant;
- liaises with school ICT technical staff, when relevant;
- receives reports of e-safety incidents and creates a log of incidents to inform future e-safety developments;
- proactively seeks to monitor evidence of radicalisation online;
- reports as appropriate to SLT

- Retain responsibility for the e-safety incident log; ensure staff know what to report and ensure the appropriate audit trail.

Roles and Responsibilities for the Network Manager/Technical staff

The Network Manager is responsible for ensuring:

- that the Trust's ICT infrastructure is secure and is not open to software based misuse or malicious attack;
- that users may only access the Trust's networks through a properly enforced password protection policy, in which passwords are regularly changed;
- the Trust's filtering policy is applied and updated on a regular basis;
- that the use of the network, remote access and email is regularly monitored in order that any misuse/attempted misuse can be reported to the E-Safety Officer for investigation/ action/ sanction;
- that monitoring software / systems are implemented and updated to take into account new developments, such as attempts to radicalise students online.

Roles and Responsibilities for the Teaching and Support Staff

Teaching and Support staff are responsible for ensuring that:

- they have an up to date awareness of e-safety matters and of the current school e-safety policy and practices;
- they have read and understood the Policies on the use of ICT and the Acceptable Use of The Internet and Trust Network;
- they report any suspected misuse or problem to the E-Safety Officer for investigation;
- digital communications with students (email / Virtual Learning Environment (VLE) / social media) should be on a professional level, in accordance with the staff code of conduct and only carried out using official school systems;
- e-safety issues are embedded in all aspects of the curriculum and other school activities;
- students understand and follow the Trust's e-safety and acceptable use policy;
- students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations;
- they monitor ICT activity in lessons, extra curricular and extended school activities;
- they are aware of e-safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices;
- in lessons where internet use is pre-planned students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches;
- monitor students' ICT usage for evidence of radicalisation and where this is seen, use school procedures to report this to the Designated Safeguarding Lead.

E-Safety Education

Teaching students to access internet content safely
Students will be taught to validate information before accepting it as true - an important aspect of higher levels of subject teaching.

E-Safety education will be provided in the following ways:

- A planned e-safety programme should be provided as part of lessons and should be regularly revisited – this will cover both the use of ICT and new technologies in school and outside school;
- Key e-safety messages should be reinforced as part of a planned programme of assemblies and tutorial activities; this will include how to report any online abuse including that related to race, religion, homophobic, biphobic and transphobic comments and how to feel safe to do so;
- Students should be taught in all lessons to be critically aware of the content they access on-line and be guided to validate the accuracy of information;
- Students should be taught to acknowledge the source of information used and to respect copyright when using material accessed on the internet;
- Students will be educated as to what radicalisation online is, how to recognise when this may be taking place, and what to do about it, when they see it.

They will be taught:

- to expect a wider range of content than can be found in the Trust's Learning Resources or on television;
- to observe copyright when copying materials from the Web;
- that the writer of an email or the author of a Web page may not be the person claimed;
- to report to a teacher immediately if they encounter any material that makes them feel uncomfortable;
- that the internet and communication technology more generally is an ever changing aspect of society and that this presents both numerous opportunities and also potential risks. Students will be taught how to protect themselves from potential risks;
- that they should not post images or videos of others without their permission;
- about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location.

Students are responsible for using the Trust ICT systems in accordance with the Acceptable Use of The Internet and Trust Network Policy, which students and their parents are expected to read before being given access to school systems. If students become aware of potential radicalisation taking place online, they should report this to a teacher.

Parents and Carers

Parents play the most important role in the development of their children; as such the Trust will provide parents with the skills and knowledge they need to ensure the safety of children outside the school environment. Through Parents' Evenings, eNews and the website, the Trust will keep parents up to date with new and emerging e-safety risks, and will involve parents in strategies to ensure that students are empowered. Parents must also understand the Trust needs have to rules in place to ensure that their child can be properly safeguarded. As such, parents must read the Acceptable Use of The Internet and Trust Network Policy before any access can be granted to school ICT equipment or services. Parents should access the Trust's website / VLE / on-line student records in accordance with the Acceptable Use of The Internet and Trust Network Policy. If parents or carers become aware of potential radicalisation taking place online, they should report this to the Trust or outside agencies such as CEOP (Child Exploitation and Online Protection Centre) or the Police.

Ensuring that internet access is appropriate and safe

The Internet is an unregulated digital forum. It is therefore not possible to guarantee that particular types of material will never appear on a device which accesses the internet within the Trust. The Trust cannot accept liability for the material accessed, or any consequences thereof. However, the following actions will be taken to ensure that the risks are minimal:

- the Trust will monitor students' usage and take all reasonable precautions to ensure that users access only appropriate material;
- a virtual learning environment will be maintained by the Trust and within this safe and controlled environment much of the online material approved by the Trust, to support students with their learning, will be stored;
- filtering software will ensure that access to undesirable sites is barred, wherever possible, and inappropriate searches are prevented;
- senior staff will ensure that occasional checks are made on files to monitor compliance with this Policy; it will be emphasised to students that their use of the internet is not private;
- staff, parents, governors and advisers will work to establish agreement that every reasonable measure is being taken;
- the CEO will ensure that the policy is implemented effectively.

Use of digital and video images – photographic, video

- When using digital images, staff should inform and educate students about the risks associated with the taking, use, sharing, publication and distribution of images. In particular they should recognise the risks attached to publishing their own images on the internet e.g. on social networking sites;
- Staff are allowed to take digital or video images to support educational aims, but must follow school policies concerning the sharing, distribution and publication of those images. Those images should only be taken on school equipment; the personal equipment of staff should not be used for such purposes;
- Care should be taken when taking digital or video images that students are appropriately dressed and are not participating in activities that might bring the individuals or the Trust into disrepute. Consent must be given by the student in accordance with the Trust's policy;
- Students must not take, use, share, publish or distribute images of others without their permission;
- Photographs published on the website, or elsewhere that include students will be selected carefully and will comply with good practice guidance on the use of such images;
- Students' full names will not be used anywhere on a website or blog, particularly in association with photographs.

Communications

When using communication technologies the Trust considers the following as good practice:

- The official school email service may be regarded as safe and secure and is monitored. Only the Trust email service, therefore, should be used to communicate with others when in school, or on school systems (e.g. by remote access);
- Users need to be aware that email communications may be monitored;
- Users must immediately report, to the Designated Safeguarding Lead, the receipt of emails that make them feel uncomfortable and/or are offensive, threatening or bullying in nature. This includes bullying of a homophobic, biphobic or transphobic nature. It is strongly advised that they do not respond to any such email;
- Any digital communication between staff and students or parents (via email or the VLE, for example) must be professional in tone and content. These communications may only take place on official (monitored) school systems. Personal email addresses, text messaging or public chat / social networking programmes must not be used for these communications;

- Students will be taught about email safety issues, such as the risks attached to the use of personal details. They should also be taught strategies to deal with inappropriate emails and be reminded of the need to write emails clearly and correctly and not include any unsuitable or abusive material;
- Personal information should not be posted on the Trust website and only official email addresses should be used to identify members of staff.
- Emailing Students - When teachers email students, this should be done via their school email address or via Google Classrooms. This ensures that the emails are logged on our server and contents can be monitored and accesses if needed.

Protection from cyber attacks
Please see the glossary of cyber terminology (at the end of this policy) to help you understand cyber security terminology.

The Trust will:

- Work with governors and the IT department to make sure cyber security is given the time and resources it needs to make the Trust secure
- Provide annual training for staff (and include this training in any induction for new starters, if they join outside of the Trust's annual training window) on the basics of cyber security, including how to:
    - Check the sender address in an email
    - Respond to a request for bank details, personal information or login details
    - Verify requests for payments or changes to information
- Make sure staff are aware of its procedures for reporting and responding to cyber security incidents
- Investigate whether our IT software needs updating or replacing to be more secure
- Not engage in ransom requests from ransomware attacks, as this would not guarantee recovery of data
- Put controls in place that are:
    - **'Proportionate'**: the Trust will verify this using a third-party audit annually to objectively test that what it has in place is up to scratch
    - **Multi-layered**: everyone will be clear on what to look out for to keep our systems safe
    - **Up-to-date:** with a system in place to monitor when the Trust needs to update its software
    - **Regularly reviewed and tested**: to make sure the systems are as up to scratch and secure as they can be
- Back up critical data daily and store these backups on [cloud based backup systems/external hard drives that aren't connected to the Trust network and which can be stored off the Trust's premises]
- Delegate specific responsibility for maintaining the security of our management information system (MIS) to our IT department
- Make sure staff:
    - Dial into our network using a virtual private network (VPN) when working from home
    - Enable multi-factor authentication where they can, on things like Trust email accounts

    - Store passwords securely using a password manager

- Make sure IT staff conduct regular access reviews to make sure each user in the Trust has the right level of permissions and admin rights
- Have a firewall in place that is switched on
- Check that its supply chain is secure, for example by asking suppliers about how secure their business practices are and seeing if they have the Cyber Essentials certification
- Develop, review and test an incident response plan with the IT department, for example, including how the Trust will communicate with everyone if communications go down, who will be contacted when, and who will notify Action Fraud of the incident. This will be reviewed and tested be at least annually though ideally every 6 months, and after a significant event has occurred, using the NCSC's 'Exercise in a Box'

Staff Training

It is the responsibility of the CEO and the Governing Body to ensure that E-Safety training for staff is regularly planned, up to date and appropriate. This will include information about CPOMS and the CEOP ThinkuKnow (http://www.thinkuknow.co.uk) resources. It is important that the wider Trust community has the knowledge to stay as risk free as possible whilst using digital technology; this includes updated awareness of new and emerging issues.

All members of staff must ensure they have read this policy in conjunction with the Acceptable Use of The Internet and Trust Network Policy.

Responding to, and Reporting of, Incidents of Misuse

It is hoped that all members of the Trust community will be responsible users of ICT, who understand and follow this policy. However, there may be times when infringements of the policy could take place, through careless or irresponsible or, very rarely, through deliberate misuse. Examples of such misuse might include:

- child sexual abuse images;
- adult material which potentially breaches the Obscene Publications Act;
- criminally racist material;
- other criminal conduct, activity or materials.

If members of staff suspect that misuse might have taken place, it is essential that the matter is brought to the attention of the E-Safety Officer and a member of the safeguarding team. They will then decide on the best way to pursue the matter. This may be through the Trust's Behaviour Policy and Safeguarding Policy although there may also be rare occasions when it will be necessary to seek the advice of the Police. Incidents will be logged on CPOMS and CEOP as appropriate. The e-Safety Officer will assist you in taking the appropriate action to deal with the incident and to fill out an incident log.

Expectation of Students

The Trust has installed computers with Internet access to help students with their learning. These rules will keep to students safe.

Students should:

- only use the Trusts ICT for schoolwork and homework.
- not damage the ICT equipment.
- only access the system with their own login and password.
- not access the internet or other networks using mobile data networks during school times.
- not access other people's files.
- not give out their home address or telephone number, or arrange to meet someone.
- report to a teacher any unpleasant material or messages sent to them. This report would be confidential and would help protect other students and individual.
- respect the interests of other people using the Internet in the same room as them, and will not deliberately access material that will distract, disturb, or offend them.
- not download or store any executable files, or any copyrighted audio or video material.
- not attempt to access network system files or software to which they do not have access rights to.
- not access any material which could be deemed inappropriate by the Trust.
- not take, share or manipulate any images or videos of students, teachers or other school members without their full consent.

Included at the end of this policy are the *E-Safety and the Acceptable Use of The Internet and Trust Network Policy – Student Agreement* and the *Chromebook and Bring your own Device Agreement.* These agreements should be signed by both students and parents

Consequences
Consequences of sending offensive messages/emails will result in in students being sanctioned in accordance with the Behaviour Policy.

Complaints
Responsibility for handling any incident that leads to a complaint, by either students or parents, will be given to the relevant Headteacher or CEO. There may be very rare occasions when the police must be contacted. Early contact will be made with relevant parties if this situation arises.

If staff or students discover unsuitable sites, the URL (address) and content will be reported to the Internet Service Provider. Any material that the Trust suspects is illegal will be referred to the Police.

Reviewed by Stone King &
ratified by Local Governors Standards Committee December 2021
Next Review: December 2026

e-Safety Incident Log

Number:	**Reported By:** *(name of staff member)*	**Reported To:** *(e.g. Head, e-Safety Officer)*	
	When:	**When:**	
Incident Description: (Describe what happened, involving which children and/or staff, and what action was taken)			
Review Date:			
Result of Review:			
Signature (Headteacher)		**Date:**	

Template Risk Log

(with a couple of examples)

No.	Activity	Risk	Likelihood	Impact	Score	Owner
1.	Internet browsing	Access to inappropriate/illegal content – staff	1	3	3	e-Safety Officer IT Support
2.	Blogging	Inappropriate comments	2	1	2	
3.	Student laptops	Students taking laptops home – access to inappropriate/illegal content at home	3	3	9	

Likelihood: **How likely is it that the risk could happen (foreseeability).**
Impact: **What would be the impact to the school (e.g. this could be in terms of legality, reputation, complaints from parents, reporting in press etc.)**

Likelihood and Impact are between 1 and 3, 1 being the lowest.
Multiply Likelihood and Impact to achieve score.

LEGEND/SCORE: 1 – 3 = Low Risk
4 – 6 = Medium Risk
7 – 9 = High Risk

Owner: **The person who will action the risk assessment and recommend the mitigation to Headteacher and Governing Body.**

Final decision rests with Headteacher and Governing Body

HASMONEAN MULTI-ACADEMY TRUST

HASMONEAN

אל תקרי בניך אלא בוניך

E-Safety and the Acceptable Use of The Internet and Trust Network Policy – Student Agreement

Note: All Internet and email activity is subject to monitoring

I will only use the Trusts ICT for schoolwork and homework.

I will not damage the ICT equipment.

I will only access the system with my own login and password, which I will keep secret. I will not access the internet or other networks using mobile data networks during school times.

I will not access other people's files.

I will use the computers only for school work and homework.

I will not give out my home address or telephone number, or arrange to meet someone- remove unless my parent, guardian or teacher has given permission.

I will report to a teacher any unpleasant material or messages sent to me. I understand this report would be confidential and would help protect other students and myself.

I understand that the School may check my computer files and monitor the Internet sites I visit.

I will – be respectful to everybody online; I will treat everybody the way that I want to be treated.

I will respect the interests of other people using the Internet in the same room as me, and will not deliberately access material that will distract, disturb, or offend them.

I will not download or store in my network user area any executable files, or any copyrighted audio or video material.

I will not attempt to access network system files or software to which I do not have access rights.

I will not access any material which could be deemed inappropriate by the School.

I will not take, share or manipulate any images or video of students, teachers or other school members without their full consent.

I will use my school email address for school related activities.

I have read the above rules and agree to follow them.

Name of Student ………………………………………………………….. (Block capitals)

Student’s signature ……………………………………Date …………………...

Parent’s signature ……………………………………Date …………………...

Signed (Parent) : **Signed (Student) :**

Date :

HASMONEAN MULTI-ACADEMY TRUST

Chromebook and Bring your own Device Agreement

Please read the following

Device Types:
For the purpose of this program, the word “device” means a Chromebook or laptop.
Guidelines:

1. The student takes full responsibility for his or her device and keeps it with himself or herself at all times or put away.
2. The student is responsible for the proper care of their personal device, including any costs of repair, replacement.
3. Hasmonean reserves the right to inspect a student’s personal device if there is reason to believe that the student has violated School policies, , school rules or has engaged in other misconduct while using their personal device
4. Violations of any school policies, administrative procedures or school rules involving a student’s device may result in the loss of use of the device in school and/or disciplinary action
5. The student complies with teacher's request to shut down the computer or close the screen or put the device away
6. The device should not be used in areas where other students could cause accidental damage in the course of their normal break time activities e.g. playing football.
7. The device is not to be used for personal reasons in school time e.g. communicating with parents
8. Personal devices shall be charged prior to bringing it to school and shall be capable of running off its own battery while at school.
9. The student may not use the devices to record, transmit or post photos or video of a person or persons on campus unless directed to do so and under supervision from a teacher. Nor can any images or video recorded at school be transmitted or posted at any time without the express permission of a teacher.
10. The student should only use their device to access relevant files, programs and/or applications.
11. The student will use the assigned wireless network. Use of 3G & 4G wireless connections is not allowed.

As a student I understand and will abide by the above Agreement and guidelines. I further understand that any violation of the above may result in the loss of my network and/or BYOD privileges as well as other disciplinary action

Name of Student ………………………………………………………… (Block capitals)

Student’s signature …………………………………Date …………………..

As a parent I understand that my child will be responsible for abiding by the above policy and guidelines. I have read and discussed it with them

Parent’s signature …………………………………Date …………………..

Signed (Parent) : Signed (Student) :

If Parents want to find out more
A guide for parents about the potential dangers facing their children on the internet, plus advice on what parents can do to help counter these hazards: https://www.gov.uk/government/publications/child-safety-online-a-practical-guide-for-parents-and-carers

Find the latest information on web sites, mobiles and new technology. Find out what's good, what's not and what you can do about it: https://www.thinkuknow.co.uk/

The UK Council for Child Internet Safety (UKCCIS) brings together organisations from industry, charities and the public sector to work with the Government to deliver the recommendations from Safer Children in a Digital World consultation: www.dcsf.gov.uk/ukccis

The Child Exploitation and Online Protection Centre (CEOP) works across the UK tackling child sex abuse and providing advice for parents, young people and children about internet safety: www.ceop.gov.uk
Or call 01482 616719 for further help and guidance.

The full guidance for Keeping children safe in education - Statutory guidance for schools and colleges September 2019 can be found by following this link - https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/835733/Keeping_children_safe_in_education_2019.pdf . Annex C specifically relates to Online Safety.

Appendix : Glossary of Cyber Security Termminology

These key terms will help you to understand the common forms of cyber attack and the measures the school will put in place. They're from the National Cyber Security Centre (NCSC) glossary.

TERM	DEFINITION
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.

TERM	DEFINITION
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (like bank details) or encouraging them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it's from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using 2 or more different components to verify a user's identity.
Virus	Programs designed to self-replicate and infect legitimate software programs or systems.
Virtual Private Network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior executives.