The Maltby Learning Trust

MLT E-Safety Policy

Date Last Reviewed:	November 2017
Reviewed by:	ICT Team Leader
Approved by:	
Next Review Due:	November 2018

Maltby Learning Trust

Statement of intent

Within the Maltby Learning Trust we understand that computer technology is an essential resource for supporting teaching and learning. The internet, and other digital and information technologies, open up opportunities for students and play an important role in their everyday lives.

Whilst the Maltby Learning Trust recognises the importance of promoting the use of computer technology throughout the curriculum, we also recognise the need for safe internet access and appropriate use.

The Trust has created this policy with the aim of ensuring appropriate and safe use of the internet and other digital technology devices by all students and staff.

The Trust is committed to providing a safe learning and teaching environment for all students and staff, and has implemented important controls to prevent any harmful risks.

This policy will operate in conjunction with other important policies in our Trust, including our Anti-Bullying Policy, Data Protection Policy, Child Protection and Safeguarding Policy.

1. LEGAL FRAMEWORK

This policy has due regard to the following legislation, including, but not limited to:

- The Human Rights Act 1998
- The Data Protection Act 1998 (GDPR General Data Protection Act 2018)
- The Safeguarding Vulnerable Groups Act 2006
- The Education and Inspection Act 2006
- The Computer Misuse Act 1990, amended by the Police and Justice Act 2006
- Communications Act 2003

2. USE OF THE INTERNET

The Trust understands that using the internet is important when raising educational standards, promoting pupil achievement and enhancing teaching and learning.

Internet use is embedded in the statutory curriculum and is therefore entitled to all pupils, though there are a number of controls required for academies to implement, which minimise harmful risks.

When accessing the internet, individuals are especially vulnerable to a number of risks which may be physically and emotionally harmful. These risks include:

- Access to illegal, harmful or inappropriate images
- Cyber bullying
- Use of social media sites and the risk of grooming
- Access to, or loss of, personal information
- Access to unsuitable online videos or games
- Loss of personal images
- Inappropriate communication with others
- Illegal downloading of files
- Plagiarism and copyright infringement
- Sharing the personal information of others without the individual's consent or knowledge

3. ROLES AND RESPONSIBILITIES

It is the responsibility of all staff to be alert to possible harm to students or staff, due to inappropriate internet access or use both inside and outside of the Trust, and to deal with incidents of such as a priority.

The Principal will act as the Academy E-Safety Officer and is responsible for ensuring the day-to-day e-safety and managing any issues within the Academy.

The CEO is responsible for ensuring that the Principal and any other relevant staff receive continuous professional development to allow them to fulfil their role and train other members of staff.

The Principal will ensure that all relevant training and advice is provided for members of staff on e-safety.

The CEO will ensure there is a system in place which monitors and supports the Principal, whose role is to carry out the monitoring of e-safety in the school.

The Principal will regularly monitor the provision of e-safety in the school and return this to the CEO.

The Trust has an established procedure for reporting incidents and inappropriate internet use, either by students or staff.

Cyber bullying incidents will be reported in accordance with the Trust's Ant-Bullying policy. The Principal will ensure that all members of staff are aware of the procedure when reporting e-safety incidents, and will keep a log of all incidents recorded.

The SRFA Committee will discuss and review the effectiveness of the e-safety provision, current issues, and to review incident logs through the risk management arrangements at the scheduled meetings.

The Trust Board will evaluate and review this E-safety Policy on an annual basis.

The CFO will review and amend this policy with the ICT Strategic Leader, taking into account new legislation and government guidance, and previously reported incidents to improve procedures.

Teachers are responsible for ensuring that e-safety issues are embedded in the curriculum and safe internet access is promoted at all times.

All staff are responsible for ensuring they are up-to-date with current e-safety issues, and this E-safety Policy.

All staff and students will ensure they understand and adhere to the Acceptable Use Policy, which they must agree to when logging onto any computer.

Parents/carers are responsible for ensuring their child understands how to use computer technology and other digital devices, appropriately.

Individual Academy Principals are responsible for communicating with parents regularly and updating them on current e-safety issues and control measures.

4. E-SAFETY CONTROL MEASURES

EDUCATING STUDENTS:

- An e-safety programme will be established and taught across the curriculum on a regular basis, ensuring students are aware of the safe use of new technology both inside and outside of the Trust.
- Students will be taught about the importance of e-safety and are encouraged to be critically aware of the content they access online.

- Students will be taught to acknowledge information they access online, in order to avoid copyright infringement and/or plagiarism.
- Clear guidance on the rules of internet use will be displayed around the Academy.
- Students are instructed to report any suspicious use of the internet and digital devices.

EDUCATING STAFF:

- All staff will have access to e-safety training and information on an annual basis to ensure they are aware of current e-safety issues and any changes to the provision of e-safety.
- All staff will employ methods of good practice and act as role models for students when using the internet and other digital devices.
- Any new staff are required to undergo e-safety training as part of their induction programme, ensuring they fully understand the E-safety Policy.

INTERNET ACCESS:

- Internet access is authorised as staff and students log on and agree to the Acceptable Use Policy.
- A record will be kept by the Principal of all students who have been granted internet access.
- All users will be provided with usernames and passwords, and are advised to keep this confidential to avoid any other students using their login details.
- Management systems will be in place to allow teachers and members of staff to control workstations and monitor students' activity.
- Effective filtering systems will be established to eradicate any potential risks to students through access to particular websites.
- Any requests by staff for websites to be added or removed from the filtering list must be first vetted by the ICT Support Team.
- All school systems will be protected by up-to-date anti-virus/malware software.
- An agreed procedure will be in place for the provision of temporary users, e.g. volunteers.

EMAIL:

- Students and staff will be given approved email accounts and are only able to use these accounts.
- Use of personal email to send and receive personal data or information is prohibited.
- No sensitive personal data shall be sent to any other students, staff or third parties via email.
- Any emails sent by students to external organisations will be overseen by their class teacher and must be authorised before sending.

- Chain letters, spam and all other emails from unknown sources should be deleted without opening them.

SOCIAL NETWORKING:

- Access to social networking sites will be filtered as appropriate.
- Should access be needed to social networking sites for any reason, this will be monitored and controlled by staff at all times and must be first authorised by the CEO.
- Students are regularly educated on the implications of posting personal data online, outside of the Trust.
- Staff are regularly educated on posting inappropriate photos or information online, which may potentially affect their position and the Trust as a whole.
- Staff are not permitted to communicate with students over social networking sites except for verified social media accounts e.g. Academy Twitter and Facebook accounts.

PUBLISHED CONTENT ON THE TRUST'S WEBSITES AND IMAGES:

- Academy Principals will be responsible for the overall content of the website, and will ensure the content is appropriate and accurate.
- All contact details on the Trust's websites will be the phone, email and address of the Academy. No personal details of staff or students will be published.
- Images and full names of students, or any content that may easily identify a student, will be selected carefully, and will not be posted until authorisation from parents has been received.
- Students are not permitted to take or publish photos of others without permission from the individual.
- Staff are able to take images, though they must do so in accordance with Trust`s policies in terms of the sharing and distribution of such. Staff will not take images using their personal equipment.

MOBILE DEVICES:

- Academy Principals may authorise the use of mobile devices by students where it is seen to be for safety or precautionary use.
- Mobile devices are not permitted to be used in the classroom by students or members of staff.
- The sending of inappropriate messages or images from mobile devices is prohibited.
- Personal Mobile devices must not be used to take images of students or staff.
- The Trust will be especially alert to instances of cyber bullying and will treat such instances as a matter of high priority.

CYBER BULLYING

- For the purpose of this policy, "cyber bullying" is a form of bullying whereby an individual is the victim of harmful or offensive posting of information or images, online.
- The Trust recognises that both staff and students may experience cyber bullying and will commit to preventing any instances that should occur.
- The Trust will regularly educate staff, students and parents on the importance of staying safe online, as well as being considerate to what they post online.
- The Trust] will commit to creating a learning and teaching environment which is free from harassment and bullying, ensuring the happiness of all members of staff and students.
- The Trust has zero tolerance for cyber bullying, and any incidents will be treated with the upmost seriousness and will be dealt with in accordance with our Anti-Bullying Policy.
- The CEO will decide whether it is appropriate to notify the police or the Director CYPS at the LA of the action taken against a student.

5. REPORTING MISUSE

MISUSE BY STUDENTS:

- Teachers have the power to discipline students who engage in misbehaviour with regards to internet use.
- Any instances of misuse should be immediately reported to a member of staff, who will then report this to the individual Academy Principal.
- Any student who does not adhere to the rules outlined in our Acceptable Use Policy and is found to be wilfully misusing the internet, will have a letter sent to their parents/carers explaining the reason for suspending their internet use.
- Members of staff may decide to issue other forms of disciplinary action to a student upon the misuse of the internet. This will be discussed with the Academy Principal and will be issued once the student is on the Trust`s premises.
- Complaints of a child protection nature shall be dealt with in accordance with our Child Protection Policy.

MISUSE BY STAFF:

- Any misuse of the internet by a member of staff should be immediately reported to the Principal.
- The Principal will deal with such incidents in accordance with the Allegations Against Staff Policy, and may decide to take disciplinary action against the member of staff.

- The Principal in consultation with the CEO will decide whether it is appropriate to notify the police or Director CYPS at the LA of the action taken against a member of staff.