MLT MIDDLESEX LEARNING TRUST

Online Safety Policy

Policy Review

This policy will be reviewed in full by the Executive Management Group (EMG) and approved by the Standards and Student Committee annually.

Chief Executive Officer:	**Ann Marie Mulkerins**
Chair of Trustees	**Gareth Jones**
MLT Policy Lead:	**Zoe Merritt**
Southgate School Policy Lead:	**Karen Burrows**
Stopsley High School Policy Lead:	**Paula Ramsay**
The Compton School Policy Lead:	**Owen Simkins**
Date approved:	**July 2023**
Review date:	**July 2024**

1. Aims

Our Trust and schools aim to:

- Have robust processes in place to ensure the online safety of students, staff, volunteers, trustees and governors
- Identify and support groups of students that are potentially at greater risk of harm online than others
- Deliver an effective approach to online safety, which empowers us to protect and educate the whole school community in its use of technology, including mobile and smart technology (which we refer to as 'mobile phones')
- Establish clear mechanisms to identify, intervene and escalate an incident, where appropriate

The 4 key categories of risk

Our approach to online safety is based on addressing the following categories of risk:

- **Content** – being exposed to illegal, inappropriate or harmful content, such as pornography, fake news, racism, misogyny, self-harm, suicide, antisemitism, radicalisation and extremism
- **Contact** – being subjected to harmful online interaction with other users, such as peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct** – personal online behaviour that increases the likelihood of, or causes, harm, such as making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography), sharing other explicit images and online bullying; and
- **Commerce** – risks such as online gambling, inappropriate advertising, phishing and/or financial scams

2. Legislation and guidance

This policy is based on the Department for Education's (DfE's) statutory safeguarding guidance, Keeping Children Safe in Education, and its advice for schools on:

- Teaching online safety in schools
- Preventing and tackling bullying and cyber-bullying: advice for headteachers and school staff
- Searching, screening and confiscation

It also refers to the DfE's guidance on protecting children from radicalisation.

It reflects existing legislation, including but not limited to the Education Act 1996, the Education and Inspections Act 2006 and the Equality Act 2010. In addition, it reflects the Education Act 2011, which has given teachers stronger powers to tackle cyber-bullying by, if necessary, searching for and deleting inappropriate images or files on students' electronic devices where they believe there is a 'good reason' to do so.

This policy complies with our funding agreement and articles of association.

3. Roles and responsibilities

3.1 The Trust Board

The Trust Board has overall responsibility for monitoring this policy and holding the CEO to account for its implementation.

The Trust Board will ensure that online safety is part of MLT schools' curricula.

The Trust Board must ensure that Trust schools have appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards which include:

- Identifying and assigning roles and responsibilities to manage filtering and monitoring systems;
- Reviewing filtering and monitoring provisions at least annually;
- Blocking harmful and inappropriate content without unreasonably impacting teaching and learning;
- Having effective monitoring strategies in place that meet their safeguarding needs.

The Trust Board delegates this responsibility to its Standards and Students Committee, who are responsible for reviewing and approving this policy.

3.2 The local governing body

The link safeguarding governor and the local governing body will make sure all staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring.

The link safeguarding governor and local governing body will also make sure all staff receive regular online safety updates (via email, e-bulletins and staff meetings/briefings), as required and at least annually, to ensure they are continually provided with the relevant skills and knowledge to effectively safeguard children.

The link safeguarding governor will discuss online safety and requirements for training at their termly meetings with the designated safeguarding lead (DSL).

The local governing body should ensure children are taught how to keep themselves and others safe, including keeping safe online.

The governor who oversees online safety is the link safeguarding governor.

All governors will:

- Ensure they have read and understand this policy

- Ensure that online safety is a running and interrelated theme while devising and implementing their whole-school approach to safeguarding and related policies and/or procedures
- Ensure that, where necessary, teaching about safeguarding, including online safety, is adapted for vulnerable children, victims of abuse and some pupils with special educational needs and/or disabilities (SEND). This is because of the importance of recognising that a 'one size fits all' approach may not be appropriate for all children in all situations, and a more personalised or contextualised approach may often be more suitable

3.3 The headteacher

The headteacher is responsible for ensuring that staff understand this policy, and that it is being implemented consistently throughout the school.

3.4 The designated safeguarding lead

Details of the school's designated safeguarding lead (DSL) are set out in our Safeguarding and Child Protection Policy, as well as relevant job descriptions.

The DSL takes lead responsibility for online safety in school, in particular:

- Supporting the headteacher in ensuring that staff understand this policy and that it is being implemented consistently throughout the school
- Ensuring the procedures and implementation are updated and reviewed regularly
- Taking the lead on understanding the filtering and monitoring systems and processes in place on school devices and school networks
- Working with the ICT manager to make sure the appropriate systems and processes are in place
- Working with the headteacher, ICT manager and other staff, as necessary, to address any online safety issues or incidents
- Managing all online safety issues and incidents in line with the Trust's Safeguarding and Child Protection Policy
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are logged and dealt with appropriately in line with the school behaviour policy
- Updating and delivering staff training on online safety
- Liaising with other agencies and/or external services if necessary
- Providing regular reports on online safety in school to the headteacher and link safeguarding governor
- Providing regular safeguarding and child protection updates, including online safety, to all staff, at least annually, in order to continue to provide them with relevant skills and knowledge to safeguard effectively

This list is not intended to be exhaustive.

3.5 The ICT manager/SLT Member responsible for ICT

The ICT manager is responsible for:

- Putting in place an appropriate level of security protection procedures, including filtering and monitoring systems on school devices and school networks, which are reviewed and updated at least annually to assess effectiveness and ensure students are kept safe from potentially harmful and inappropriate content and contact online while at school, including terrorist and extremist material
- Ensuring that the school's ICT systems are secure and protected against viruses and malware, and that such safety mechanisms are updated regularly
- Blocking access to potentially dangerous sites and, where possible, preventing the downloading of potentially dangerous files
- Ensuring that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy

This list is not intended to be exhaustive.

3.6 All staff and volunteers

All staff are responsible for:

- Maintaining an understanding of this policy
- Implementing this policy consistently
- Agreeing and adhering to the terms on acceptable use of the school's ICT systems and the internet (appendix 1), and ensuring that students follow the school's terms on acceptable use (appendix 2)
- Knowing that the DSL is responsible for the filtering and monitoring systems and processes, and being aware of how to report any incidents of those systems or processes failing
- Following the correct procedures if they need to bypass the filtering and monitoring systems for educational purposes
- Working with the DSL to ensure that any online safety incidents are logged and dealt with appropriately in line with this policy
- Ensuring that any incidents of cyber-bullying are dealt with appropriately in line with the school behaviour policy
- Responding appropriately to all reports and concerns about sexual violence and/or harassment, both online and offline, and maintaining an attitude of 'it could happen here'

This list is not intended to be exhaustive.

3.7 Parents

Parents are expected to:

- Notify the school of any concerns or queries regarding this policy

- Ensure their child has read, understood and agreed to the terms on acceptable use of the school's ICT systems and internet (appendix 2)
- Parents can seek further guidance on keeping children safe online from the following organisations and websites:
- What are the issues? - UK Safer Internet Centre
- Hot topics - Childnet International
- Parent resource sheet - Childnet International

3.7 Visitors and members of the community

Visitors and members of the community who use the school's ICT systems or internet will be made aware of this policy, when relevant, and expected to read and follow it.

4. Curriculum and training

- Online safety taught to all students in years 7-13 through the pastoral/PSHE curriculum to ensure that students are taught how to keep themselves and others safe online.

- Online safety information, training and advice is provided to parents through information evenings and newsletters. The information shared with parents will include what systems the school uses to filter and monitor online use and what their children are asked to do online, including the sites they will be asked to access and who from the school their child will be interacting with online

- All staff undergo online safety training as part of child protection and safeguarding training, and ensure staff understand their expectations, roles and responsibilities around filtering and monitoring

- DSL and DDSLs receive training in the unique risks presented by online safety and are mindful of the increased risks to specific groups of students, e.g. students on the SEND Register.

5. Related Policies

MLT Complaints Policy
MLT IT & Cyber security policy
MLT Data Protection Policy
Schools' Positive Behaviour Policy
MLT Safeguarding and Child Protection Policy
MLT Staff Conduct Policy
School Exams policy

Appendix 1: MLT Computer and Internet Acceptable Use Policy for Staff
Appendix 2: MLT Computer and Internet Acceptable Use Policy for Students

Appendix 1

MLT Computer and acceptable use policy for staff

This policy is designed to enable acceptable use for staff and governors. All staff having access to the networks must sign a copy of this Computer and Internet Acceptable Use Policy.

The School provides a range of ICT resources which are available to staff members and governors. In order to ensure the safety of staff, governors and students, it is important that all staff members and governors follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the School's ICT systems and infrastructure.
- Define and identify unacceptable use of the School's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and school devices.
- Specify the consequences of non-compliance.

This policy applies to staff members and governors, and all users of the School's ICT systems are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of this policy may result in disciplinary action.

The use by staff and monitoring by the School of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the School's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the SLT Member responsible for ICT Systems.

Provision of ICT Systems

All equipment that constitutes the School's ICT systems is the sole property of the School.

No personal equipment should be connected to or used with the School's ICT systems without the permission of the IT network manager or SLT member responsible for ICT systems. Users must not install any software on the ICT systems without permission from the IT network manager. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

The SLT Member responsible for ICT systems is responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time, without prior warning, for regular maintenance, reallocation or any other operational reason. Maintenance includes, but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Network Access and Security

Users are not permitted to make any physical alteration, either internally or externally, to the School's computer and network hardware.

All users of the ICT systems at the School must first be registered. Following registration, a network user account will be created, consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security and comply with guidelines laid out in the MLT IT and Cyber Security Policy. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them to any other person, except to designated members of the IT Network team for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to the IT Network manager and SLT member responsible for ICT Systems as soon as possible.

Users should only access areas of the school's computer systems to which they have authorised access. Under no circumstances should a pupil be allowed to use a staff computer account, unless being directly supervised by the account owner.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the School ICT systems, or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the School ICT systems or cause difficulties for any other users. Further guidance on maintaining network security can be found in the MLT Cyber Security policy

School Email

Where email is provided, it is for academic and professional use, with no personal use being permitted. The School's email system can be accessed from both the School computers, and via the internet from any computer. All School related communication must be via the School email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, or be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the School does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official school business is not permitted.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g. sensitive or personal information) will only be sent using a secure method including:
    - Email encryption;
    - A secure upload portal (where by the recipient will be required to log in to retrieve the email/documentation sent);

  - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e. in a separate email or over the phone).
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible.
- Access to school/setting email systems will always take place in accordance to data protection legislation and in line with other appropriate school/setting policies e.g. confidentiality.
- Members of the community must immediately tell the SLT member responsible for ICT Systems if they receive offensive communication, who may refer the matter to the school's designated safeguarding lead.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on school headed paper would be.
- School email addresses and other official contact details will not be used for setting up personal social media accounts.
- Emails must not contain personal opinions about other individuals, e.g. other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.

Internet Access

Internet access is provided for academic and professional use, Personal use should be limited to short periods during recognised break times and comply with this Acceptable Use Policy. The School's internet connection is filtered, meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is inappropriate for use in a school. In this case the website must be reported immediately to a member of the IT Network team or the SLT Member responsible for ICT systems.

Staff must not therefore access from the School's system any web page or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may, in certain circumstances, constitute a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material, or using any of the following facilities, will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials;
- transmitting a false and/or defamatory statement about any person or organisation;
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others;
- transmitting confidential information about the School and any of its staff, students or associated third parties;
- transmitting any other statement which is likely to create any liability (whether criminal or civil, and whether for the employee or for the School);
- downloading or disseminating material in breach of copyright;
- engaging in online chat rooms, instant messaging, social networking sites and online gambling;
- forwarding electronic chain letters and other materials;
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the School may undertake a more detailed investigation in accordance with the MLT Staff Code of Conduct involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Approved Software

The school's IT team provides a range of software for use within the school. Some of this software will be installed locally on school devices while other systems will be hosted and accessible via the cloud. Should staff wish to utilise additional software or apps, requests should be made via the school IT Team. Staff should not install unapproved software or apps onto school devices. Staff should also not sign up to cloud-based software for school use without prior approval.

Digital Cameras

The School encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Photos should only have the student's name if they are on display in school only. Photos for the website or press must only include the child's first name.
- All photos should be downloaded to the School network as soon as possible.
- If staff use the cameras on their mobile phones to document trips and events, consent from staff and students must be sought and the images must be stored on the school network and deleted from staff member's device within 24 hours.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives and cloud storage. Any school related work should be stored on one of these drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file stored in their area, for example copyright music files.

Any files stored on removable media must be stored in accordance with the MLT Data Protection and IT/Cyber Security Policies, summarised as follows:

- Sensitive school data should not be stored on or transferred by removable storage devices such as USB Drives.
- No school data is to be stored on a home computer, or un-encrypted storage device.
- No confidential, or school data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email

Mobile Phones

Mobile phones are permitted in school, however are not to be used for personal use while working with or in contact with students.

All phone contact with parents regarding school issues will be through the School's phones. Personal mobile numbers should not be given to parents at the School.

Use of WhatsApp

WhatsApp and similar personal messaging services are not permitted for use on school issued devices or personal devices for school business. Members of staff are able to use such messaging services on their own devices for personal communication however, staff should not communicate internally with other staff members for school business using their personal accounts.

Use of Social media

When using social media staff must be aware of the following requirements for staff are as follows:

- Staff members have a responsibility to protect the reputation of the School, staff and students at all times and must treat colleagues, students and associates of the School with professionalism and respect whilst using social networking sites.
- Social networking sites should be used responsibly, and users should ensure that neither their personal or professional reputation and/or the School's reputation, nor the reputation of individuals within the School are compromised by inappropriate postings.
- Use of social networking sites for school business is not permitted, unless via an officially recognised school site and with the permission of the SLT Member responsible for Media and Communications.
- Members of staff will notify the SLT Member responsible for Media and Communications if they consider that any content shared or posted via any information and communications technology, including emails or social networking sites conflicts with their role in the School/setting.
- No school information, communication, documents, videos and/or images should be posted on any personal social networking sites.
- No details or opinions relating to any pupil are to be published on any website.
- Users must not knowingly cause annoyance, inconvenience or needless anxiety to others (cyber bullying) via social networking sites.
- No opinions regarding another member of staff, which could cause offence, are to be posted.
- No photos or videos, which show pupils of the School who are not directly related to the person posting them, should be uploaded to any site other than the School's Website.
- No comment, images or other material may be posted anywhere, by any method that may bring the School or, the profession into disrepute.
- Users must not give students access to their area on a social networking site, (for example adding a student as a friend on Facebook).

Monitoring the use of ICT Systems

The School may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the School's ICT system is, or may be taking place, or the system is, or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is

installed to ensure that use of the network is regularly checked by the IT network manager to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.
Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided;
- maintain the systems;
- prevent a breach of the law, this policy, or any other school policy;
- investigate a suspected breach of the law, this policy, or any other school policy.

Any unauthorised use of the School's ICT systems, Cloud-based ICT systems, the internet, e-mail and/or social networking site accounts, which the SLT Member responsible for ICT Systems considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority.
The School reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Failure to Comply with Policy

Any failure to comply with the policy may result in disciplinary action. Depending upon the severity of the offence, a breach of this policy may be considered gross misconduct leading to summary dismissal.

ACCEPTABLE USE AGREEMENT

To be completed by all staff

As a school user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the School rules (set out within this policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the School Acceptable Use Policy. If I am in any doubt, I will consult the SLT Member responsible for ICT systems.

I agree to report any misuse of the network to the SLT Member responsible for ICT systems Moreover, I agree to report any websites that are available on the School internet that contain inappropriate material to the IT Network Team. I finally agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the SLT Member responsible for ICT systems.

Specifically, when using school devices:

- I must not use these devices for inappropriate purposes;
- I must only access those services for which permission has been granted;
- I will not download, use or upload any material which is unsuitable within a School setting or that may cause disruption to the School network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the School will monitor communications in order to uphold this policy and to maintain the School's network (as set out within this policy).

Appendix 2

The MLT Computer and Internet Acceptable Use Policy

For Students

All parents of students having access to the networks must sign a copy of this Computer and Internet Acceptable Use Policy and return it to the School Office.

The computer network is owned by the school and is made available to students to further their education. The school's Computer and Internet Acceptable Use Policy has been drawn up to protect everyone and failure to comply with this policy will result in you not being able to use school computers or more serious sanctions in accordance with the ICT Sanctions.

- Students must only access the network and Internet via their authorised account and password. Students must not make this information available to any other person**.**
- Students are only allowed to use the network computers when a member of staff is present.
- The school reserves the right to examine and / or delete any files that may be held on its computer network and / or to monitor any Internet sites visited or e-mails sent or received.
- Users may not install, or attempt to install, their own software; nor may they delete or attempt to delete system software, alter another user's files.
- Students must not perform a function with the intent to gain unauthorised access to any programs, files or data held on the computer.
- Activity which threatens the integrity of the school IT systems ('hacking'), or activity which attacks or corrupts other systems, is forbidden.
- Users must not attempt to repair or rearrange the hardware and any such issues should be referred to the IT Systems and Network manager.
- The cost of replacement or repair for any damage caused through neglectful or irresponsible behaviour or acts of vandalism or will be charged to the individual concerned.

All Internet activity must be appropriate to the student's education.

- The use of chat rooms and social networking sites is not allowed and appropriate action will be taken.
- Students may not download music files to the school network and the sharing of music files is strictly forbidden.
- Use of the network to access inappropriate materials such as pornographic, racist or offensive material are forbidden and appropriate action will be taken.
- Students must not use proxy websites to gain access to banned web material.
- Use of the school's network for financial gain, gambling, political purposes or advertising is forbidden.
- Copyright and intellectual property rights must be respected.
- Plagiarism or copying of others work is strictly forbidden
- Students must report any accidental access to, or receipt of inappropriate materials, or filtering breach to their teacher.

- Any students given permission to bring their own digital/ mobile device into school must use the school wi-fi network. All devices are registered and usage is monitored the same as the school IT network.
- Any hurtful, threatening comments made on-line or via a mobile phone within school or out of school will be considered to be bullying and dealt as per the school behaviour policy.

ALL SCHOOL NETWORK, INTERNET AND MANAGED LEARNING ENVIRONMENT SYSTEMS ARE MONITORED AND WE RESERVE THE RIGHT TO EXAMINE ANY AREA OF THESE SYSTEMS.

The use of computer systems without permission or for inappropriate purposes could be a criminal offence under the Computer Misuse Act 1990 (The Computer Misuse Act 1990 makes it a criminal offence to “cause a computer to perform any function with intent to secure unauthorised access to any program or data held in any computer”. Sending malicious or threatening e-mails and other messages is a criminal offence under the Protection from Harassment Act (1997), the Malicious Communications Act (1988) and Section 43 of the Telecommunications Act (1984).)

I have read and understood the Policy above, and agree to the conditions stated. I understand that my access to the network may be restricted or denied if I knowingly contravene any of these conditions. I have also read and agree to the attached ‘Rules and Responsibilities for Computer and Internet Use’.

Student Print Full Name ……………………………………. Signed…………………………Date

Parent Print Full Name …………………………………... Signed ……………………… Date