Trust E-Safety and Social Media Policy

June 2021

Contents

1. RATIONALE

Within the Education and Leadership Trust (ELT), we believe that the use of technology is an essential part of education in the 21st century. We are immersed in a digital world where information is available 24 hours a day, 7 days a week. The internet, social media platforms and other digital and information technologies are powerful tools, which open new opportunities for everyone. These technologies can be used to encourage discussion, provide outlets for creativity and enrich the curriculum. The use of e-mail, mobile phones, internet messaging, social media and blogs can all enable improved communication on an unprecedented scale and our remote learning system(s) offer a platform for personalised and independent learning, on demand.

In addition to these benefits, however, there are risks and unfortunately some adults and young people may expose themselves to danger either knowingly or unknowingly. In the light of the rapid evolution of IT systems and social networking technologies, the Trust requires a robust policy framework so that all adults working in the academies are aware of the Trust's expectations and the rules they are expected to follow when using IT equipment and systems and social media platforms both inside and outside of the academy environment.

It is crucial that whilst promoting the positive use of technology in our academies, we recognise the potential risks and take steps to protect our students, staff and visitors so that staff and children are safeguarded and that parents, students and the public at large have confidence in the Trust's decisions and services. Responsible use of social media will ensure that the confidentiality and privacy of students and members of staff are maintained and that the reputation and integrity of the academies and the ELT are protected.

2. PURPOSE OF THE POLICY

This policy defines the expectations for the use of IT for staff at the Education and Leadership Trust (ELT). Its purpose is to: support the use of IT for effective working and communication; encourage the creative use of technology to engage learners; minimise the risks to students and staff of inappropriate situations and materials; protect the staff and academy from litigation and to minimise the risks to the IT network and systems. It is designed to ensure that all adults use IT equipment, services and social media platforms responsibly in order to safeguard the Trust, the individual academies, students, staff, academy governors, Trustees and members of the wider academy communities.

This policy should be read in conjunction with other relevant Trust and academy policies in particular, the Trust's Safeguarding Policy, Code of Conduct and Disciplinary Policy

This policy takes into account the provisions of the DfE's statutory advice for academies (September 2021) on Keeping Children Safe in Education, the non- statutory guidance on the Prevent Duty (June 2015), and the Briefing Note to academies on "How Social Media is used to encourage travel to Syria and Iraq". It also takes into account the Government's statutory guidance issued under s29 of the Counter -Terrorism and Security Act 2015 (June 2015).

The principles which underpin this policy are:

- The Trust is committed to utilising technology to support learning and working practices.
- Adults are responsible for their own actions and behaviour and must avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Adults must continually monitor and review their own practices in terms of the continually evolving world of technology, systems and social networking and ensure that they consistently follow the rules, principles and guidance contained in this policy.
- The rapid developments in hardware and software mean that use of technology changes at an unprecedented rate. It would be impossible to document every potential use of IT equipment and services therefore, in order to remain flexible, use of IT within the Education and Leadership Trust is underpinned by the term 'Unacceptable Use'.

3. SCOPE AND DEFINITIONS

This policy applies to all adults working for the ELT and who provide services for or on behalf of the academy including employees (teaching and non-teaching staff), trainee teachers and any other trainees, apprentices, self-employed staff, agency staff, external consultants and volunteers. This policy also applies to Trust and academy governors and Trustees.

This policy deals with the use of IT facilities and associated web-based services across the Trust, external systems (including social media platforms), academy owned devices, personal devices used for academy or Trust related use and applies to all academy employees, and authorised users. It covers the personal use of social media as well as the use of social media for professional use and/or academy purposes (whether official or not), including the use of websites and services hosted and maintained on behalf of the academy.

This policy covers the use of IT equipment and social media as defined in this policy and also personal blogs and any posts made on other people's blogs and to all on line forums and notice boards. The guidance, rules and principles set out in this policy must be followed irrespective of the device, social media platform or medium.

In this policy, the following definitions apply:

- **unacceptable use** - is defined as any activity which is; conducted without permission, outside the specific learning aim for that lesson or activity, illegal, considered extreme or radicalising, dangerous, vexatious or where the equipment is used to make any student, member of staff or member of the public feel uncomfortable or vulnerable.
- **IT equipment and services** – means any device, network, software system or other digital resource used for academy or Trust related business irrespective of the ownership of that device.
- **personal use** - means any activity, account or system used privately for home, leisure or other interests which do not relate to the academy, the rust or business other than education.

- **professional use** - means any activity, account or system that is used for any business related to education, employment area or where you are maintaining a presence in a professional capacity.
- **Trust use** – means any account set up on behalf of the Trust, an academy, a department or an individual which is designed to reflect the opinions and values of the academy or the Trust.
- **social media/social networking platforms** - means any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. Social media includes but is not limited to, online social forums such as Twitter, Facebook and LinkedIn and also covers blogs, chat rooms, forums, podcasts and video-image-sharing websites such as YouTube, TikTok, Snapchat, Instagram, Reddit, Instagram, Pinterest and Tumblr. (The internet is a fast-moving technology and it is impossible to cover all examples of emerging social media in this policy.)
- **adults/adults working in academy** - means all members of staff (including teaching and non-teaching staff) who work for the Education and Leadership Trust as an employee or on a self- employed basis. It also includes trainee teachers, other trainees and apprentices, volunteers, agency staff, external consultants and academy governors.
- **information** - means all types of information including but not limited to, facts, data, comments, audio, video, photographs, images and any other form of online interaction.
- **inappropriate information** - means information as defined above which any reasonable person would consider to be unsuitable or inappropriate in the circumstances and considering the adult's position within the academy.
- **the Trust, the academy and the wider academy community** - means the Education and Leadership Trust, any academy designated as part of the Trust, any pupil, parents/carers of students, former students of any academy in the Trust, any adult that is, or has been, employed by the Education and Leadership Trust and any other person or body directly or indirectly connected with the Trust or any of its member academies.

4. ROLES AND RESPONSIBILITIES

The Trust Board is responsible for ensuring that its employees, governors and Trust directors act in a lawful manner, making appropriate use of academy technologies for approved purposes only.

The Trust Board or delegated group is responsible for overseeing relevant policies and the Headteacher is responsible for ensuring that staff are aware of their contents.

The Headteacher is responsible for ensuring an inventory of IT equipment is recorded as part of the academy asset management register.

If the Headteacher or Executive Headteacher has reason to believe that any IT equipment has been misused by an adult, they will consult the Trust's HR Director for advice without delay. The HR Director will agree with the Headteacher or Executive Headteacher an appropriate strategy for the investigation of the allegations and liaison with other agencies as appropriate. Incidents will be investigated in a timely manner in accordance with agreed procedures. The Headteacher and Executive Headteacher will make it clear that internal academy staff should not carry out any investigations unless they are both qualified and authorised to do so.

The Headteacher and the Trust will:

- provide IT equipment and services with appropriate functionality and security mechanisms and ensure that all adults working in academy are familiar with this policy and any related policies.
- take all reasonable steps to enable adults to work safely and responsibly and to support safer working practice in general with regard to the use of the IT equipment and services, the internet and other communication technologies.
- ensure appropriate filters and monitoring systems are in place.
- set clear rules in relation to the expected standards of behaviour whilst using relevant IT equipment and services and social networking platforms for personal, professional or Trust use.
- give a clear message that unlawful or unsafe behaviour or practice is unacceptable and that where appropriate, disciplinary, legal and/or other action will be taken.
- ensure that all concerns raised in relation to the misuse of Trust or academy IT equipment and services, and social media sites are investigated promptly and appropriately.
- ensure procedures are in place to handle allegations against any adult.
- take all reasonable steps to minimise the risk of misplaced or malicious allegations being made against adults working in academy.
- take all reasonable steps to prevent adults working in academy abusing or misusing their position of trust.

Adults working in academy must:

- ensure they are familiar with the contents of this policy and the accompanying guidance.
- adhere to and apply the rules, guidance and principles in this policy in all aspects of their work and in their personal time.
- act in accordance with their duties and responsibilities under this policy and the statutory/ non statutory advice and guidance referred to.
- demonstrate high standards of personal and professional conduct when using IT equipment and services, and social media platforms.
- only use the IT equipment and services for which they have authorisation.
- use IT equipment and services only for their intended purpose.
- use appropriate channels of communication and pay regard to the information being communicated.
- take reasonable steps to protect the access and integrity of all IT equipment and services.
- respect the privacy and personal rights of others.
- never, in any circumstances, abuse or misuse their position of trust.
- raise any concerns or queries in connection with this policy with the academy Headteacher.
- be alert for signs of cyber-bullying, exploitation or radicalisation and report concerns immediately through the appropriate academy systems.
- engage with any training provided or facilitated by or the academy in relation to the use of the internet or any other digital or communication technologies.

Key personnel	**Whalley Range**	**Levenshulme**	**TEMA**
E-safety Lead	Mrs Catherine Wragg	Mrs Catherine Wragg	Mrs Catherine Wragg
Designated Safeguarding Lead	Ms Morresa Connolly	Ms Donna Johnson	Mr David Goddard

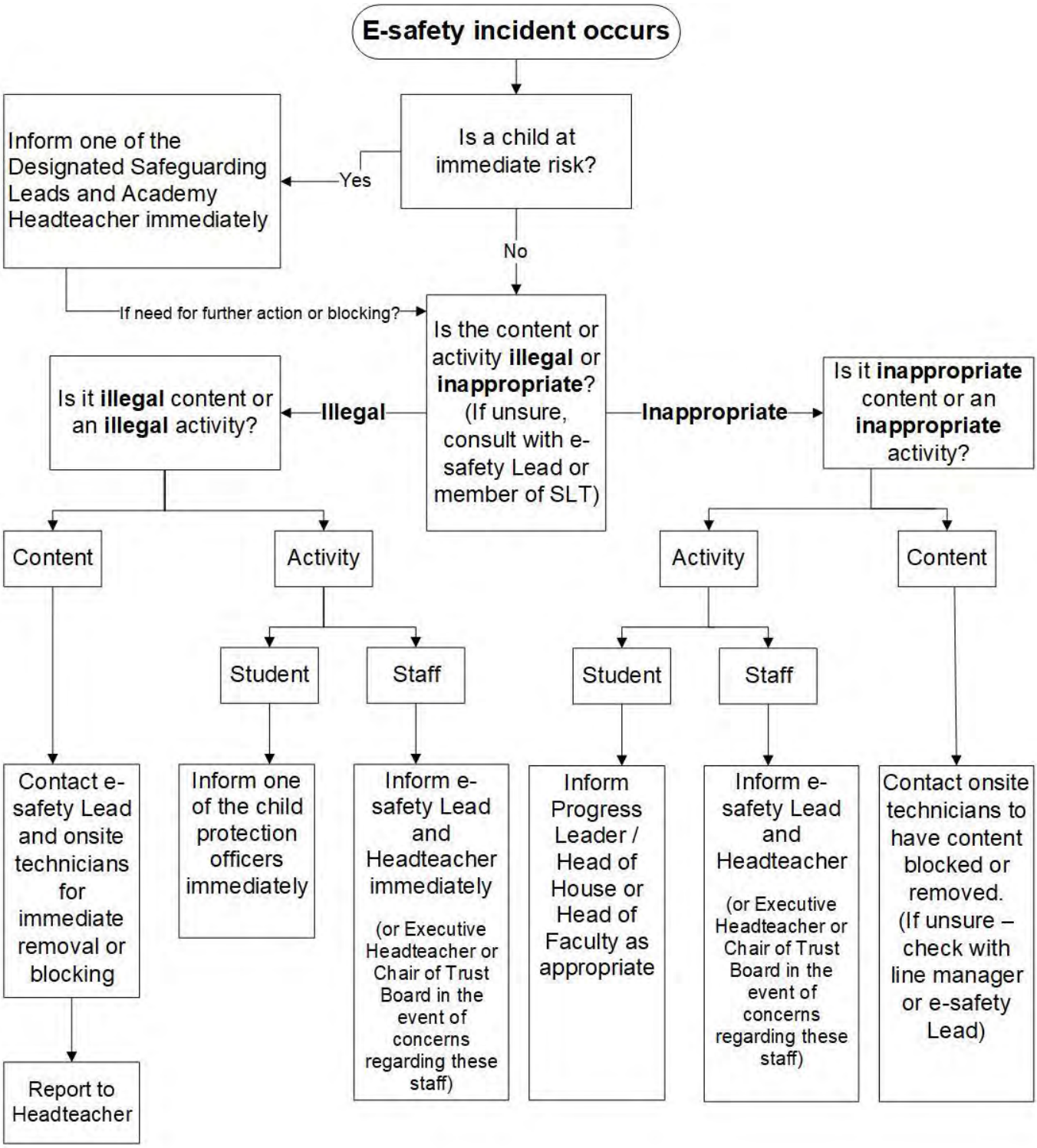
The policy must be read in conjunction with the Data Protection Policy, the Safeguarding Policy, the E-safety guidance and the Staff Code of Conduct

5. REPORTING

Staff are responsible for reporting every breach of e-safety. If a member of staff knows, or suspects, that a colleague is in breach of any part of this policy he/she must report it to the appropriate person in writing by email to the following leads and copy in the academy Headteacher.

It is also important to recognise that e-safety is not an IT issue. It may involve the use of IT, but it is about protecting children and young people from harm If a me. This policy relates to staff but the reporting mechanisms outlined below also relate to students for clarity and ease of use. If a member of staff has concerns about the behaviour of a young person in relation to IT systems or services they should follow the mechanisms outlined in the Safeguarding policy. If you have a concern about actual, significant harm to a child or young person, or the risk of significant harm, then you should make immediate contact with the Child Protection Officers in academy.

Timescale:	**Incident:**	**Report to:**	**Method**
Immediate reporting:	Illegal activity by student or illegal content viewed by student	Child Protection Team	CPOMS
	Illegal or inappropriate activity by a member of staff	Headteacher and e-safety Lead	Email
	Illegal or inappropriate activity by the Headteacher	Executive Headteacher	Email
	Illegal or inappropriate activity by Executive Headteacher	Chair of Trust Board	Email
	Illegal content or material which requires **immediate** removal or blocking	Onsite technicians and e-safety Lead	Email
Same day reporting:	Inappropriate material which requires additional filtering on the internet	Onsite technicians and e-safety Lead	Email
	Inappropriate activity by a student in a lesson (which does not constitute a child protection incident)	Heads of Faculty/Subject or Pastoral Leaders as appropriate to the behaviour policy	SIMS
	Inappropriate activity by a student not in a lesson (which does not constitute a child protection incident)	Heads of House / Year / Progress Leaders as appropriate to the behaviour policy	SIMS



Any incident involving a concern about a student must be formally recorded on CPOMS and/or SIMS. The headteacher or appropriate senior staff will make the decision about contact with parents.

Any incident concerning a member of staff must be reported by email to the appropriate person

6. BREACHES OF POLICY AND OTHER ISSUES

- Any breach of this policy and the duties, responsibilities, professional standards and legal obligations referred to will be regarded as a serious matter and action including disciplinary action in appropriate circumstances will be taken by the Headteacher (or the Academy Committee or Trust Board). In serious cases involving employees this may lead to dismissal without notice on the grounds of gross misconduct.

- Where there has been a breach of this policy, the academy will also take whatever action is considered appropriate in order to protect the reputation and integrity of the academy, the Trust and the wider academy community.

- Adults must be aware that any breach of this policy involving a breach of the laws, professional codes or other statutory provisions referred to in this policy may result in legal or other action being taken against them by a body or person other than the academy.

7. FURTHER INFORMATION AND GUIDANCE

- Information relating to the use of IT equipment and services, and social media is published in a separate document.
- Electronic guides and training is available via the links on the academy Intranet
- Further clarification can be requested by contacting the e-safety Lead cwragg@eltrust.org