Online Safety Policy

Document Control

Version	Author	Summary of Changes	Approved By	Date Published	Date of Review
V1	RGR	New Policy	Finance and Operations Committee	May 2021	May 2023
V2	MPI	Changes to 4.3.3. 5.4 Update re DSL	Finance and Operations Committee	May 2023	May 2025
V3	RGR/MPI	Update job titles	CEO	May 2025	May 2028

Contents

1. INTRODUCTION

1.1. Leger Education Trust is committed to promote the welfare and safety of our students in all of our academies when using digital and online technologies. LET recognises the importance of the contribution it can make to protecting and supporting students across its academies in their use of these technologies.

1.2. This policy is designed to incorporate all aspects of child protection and safeguarding that may be affected by digital technology, mobile phone technology, as well as LET's use of technology with its academies.

1.3. The organisation will refer to the most recent government, Department for Education (DfE) and Information Commissioners Office (ICO) guidance and documentation with regard to data protection, data storage and privacy compliance.

2. SCOPE

2.1. This policy applies to all LET staff (including agency), pupils/students, parents/carers, Trustees, Ambassadors and other volunteers.

2.2. This policy applies to any individual who is given access to LET's digitally connected systems (including email addresses and any other data source or system that is hosted/operated/controlled remotely or other by the organisation).

2.3. LET expects all academies will make reasonable use of relevant legislation and guidelines to affect positive behaviour regarding the use of technology and the Internet both on and off the school site. This will include imposing rewards and sanctions for behaviour - as defined as regulation or student behaviour under the Education and Inspections Act 2006. The 'In Loco Parentis' duty allows the academy to report and act on instances of cyber bullying, abuse, harassment (including sexual harassment), malicious communication and grossly offensive material; including reporting to the police, social media websites, and hosting providers on behalf of pupils.

2.4. The Online Safety Policy covers the use of:

- School based IT systems and cloud-based software;
- School based intranet and networking;
- School related external Internet, including but not exclusively e-learning platforms, blogs, social media websites;
- External access to internal school networking, such as webmail, network access, file serving (document folders) and printing;
- School IT equipment off-site, for example staff laptops, digital cameras, mobile phones, tablets, dongles;
- Student and staff personal IT equipment when used in school and which makes use of school networking, file-serving or Internet facilities;
- Tablets, mobile phones, devices and laptops when used on the academy site.
- http://www.legislation.gov.uk/ukpga/2006/40/contents4

3. POLICY STATEMENT

3.1. The definition of an online incident is:

"Any incident that occurs and involves any person (student or adult) where the use of technology (equipment and/or networks) enables or facilitates inappropriate behaviour and harm and/or distress is caused to another person or the reputation of the Academy and/or LET. This may include the use of social media, forums, blogs, open and closed groups, digital images, messages or any other means".

3.2. The most likely areas of risk to students are:

- Exposure to illegal inappropriate or harmful material;
- Subject to harmful online interactions with other users;
- The individual's personal online risky behaviour that then leads to harm.

3.3. LET has a responsibility for ensuring that the resources are available to promote the safe use of technology and to promote understanding and awareness of the risks attached to the use of digital technology.

3.4. We seek to promote the use of technology and connectivity to ensure that the students are equipped with the necessary skills and knowledge to perform to the best of their ability both during their time in their academy and also in their future in their chosen careers and workplaces.

3.5. Staff and students must be able to use digital technology appropriately and safely and understand the risks related to their activity. Students will receive online safety education as soon as they start using digital technology and this will be continually reinforced and monitored as students' progress through their school life.

3.6. LET actively encourages a proactive approach to new and emerging technologies and threats to mitigate the risk of harm to students, staff and the Trust and associated academies and their reputations. We seek to promote a 'cyber aware' culture that ensures all staff, students and trustees take part in and continue to develop their knowledge and understanding of online behaviour and in particular, how to prevent harm through continual learning resources, research and encouragement from all teachers.

4. STANDARDS AND EXPECTATIONS

4.1. Systems

4.1.1. Academy computer systems will be configured to ensure the teaching and learning requirements of the academy are met whilst ensuring online safety is maintained.

4.1.2. Risk assessments and Data Privacy Impact Assessments (DPIA) are completed when there is a major overhaul to the system or a new cloud-based software package is purchased, for example.

4.1.3. The system will be compliant with the academy, Trust, local authority, DfE, ICO and Data Protection guidelines with regard to online safety procedures being met.

4.1.4. Regular audits and evaluations of the IT network will be carried out, identifying where improvements can be made.

4.1.5. Trust IT staff will be responsible for monitoring IT use.

4.2. Filtering

4.2.1. The academy will ensure an accredited filtering system is used. Filtering reports and logs will be examined regularly.

4.2.2. Any filtering incidents are examined and action taken and recorded to prevent a reoccurrence. The academy will provide enhanced/differentiated user-level filtering. Internet access will be filtered for all users.

4.3. Network security

4.3.1. All users will have clearly defined access rights to academy technical systems and devices.

4.3.2. All users will be provided with a username and secure password by Trust IT staff. Users are responsible for the security of their username and password.

4.3.3. The Director of IT & IT Manager and when required other designated senior person will have access to the main administrator passwords.

4.3.4. Appropriate security measures are in place to protect the servers, firewalls, routers, wireless systems, workstations etc. from accidental or malicious attempts which might threaten the security of the academy systems and data.

4.4. Use of images and videos

4.4.1. The academy will ensure images and videos of students, staff, students' work and any other personally identifying material are used, stored, archived and published in line with the Data Protection Act, ICO guidance for schools, DfE guidance for schools and the Acceptable Use Policy.

4.4.2. 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 the risks attached to publishing their own images on the Internet e.g. social media sites.

4.4.3. Written permission from parents or from LET will be obtained before photographs of students are published on the school website/social media/local press.

4.4.4. In accordance with guidance from the ICO, parents are able to take videos and digital images of their children at academy events for their own personal use, but should not be made publicly available where other students are involved in the digital image or video.

4.4.5. Students must not take, use, share, publish or distribute images of others without their permission.

4.5. Data Protection

4.5.1. Personal data will be recorded, processed, transferred and made available according to the Trust Data Protection Policy and in compliance with GDPR and the Data Protection Act (2018).

4.6. Social Media

4.6.1. Trustees, academy, national and regional team staff, students and volunteers are expected to comply with the Trust's Social Media Policy.

5. RESPONSIBILITIES

5.1. Headteachers should ensure that all academy staff and visitors are aware of the Online Safety Policy and procedure and of their responsibilities set out in this policy. It is the responsibility of the Headteacher to ensure that breaches of the policy are investigated and addressed.

5.2. Academy staff, Trust staff and Trustees are expected to adhere to the policy and procedure and ensure that they conduct themselves in a manner that will not place students or vulnerable adults at risk, bring the school into disrepute or damage their own professional reputation.

5.3. Academy management and online safety

5.3.1. Academy Senior Leadership Teams (SLTs) are responsible for determining, evaluating and reviewing online safety to encompass teaching and learning, use of academy IT equipment and facilities by students, staff and visitors, and agreed criteria for acceptable use by students, school staff and trustees of Internet capable equipment for academy related purposes, or in situations which will impact on the reputation of the academy, and/or on academy premises.

5.3.2. Regular assessment of the strengths and weaknesses of practice within the academy will help determine INSET provision needed for staff and guidance provided to parents, students and local partnerships.

5.4. Online Safety Co-ordinator

5.4.1. The academy Designated Safeguarding Lead (DSL) will act as the Online Safety Co-ordinator who coordinates online safety provision across the academy and wider school community.

5.4.2. The academy's Designated Safeguarding Lead (DSL) is responsible for online safety issues on a day to day basis and also liaises with relevant stakeholders including IT support and other Trust contacts, to ensure the safety of students.

5.5. Trustees

5.5.1. The Trustees delegate a number of functions to the Executive Director of Operations, Director of IT and Academy SLT. The Designated Safeguarding Leads, on behalf of the Board of Trustees, will liaise directly with one another with regard to reporting on online effectiveness, incidents, monitoring, evaluation to the Director of IT and Headteachers, developing and maintaining links with local stakeholders and wider academy community.

5.5.2. This is important also to provide and evidence a link between the academy, trustees and parents.

5.5.3. Designated Safeguarding Leads must ensure that they have demonstrable experience, skills and training to be able to provide appropriate challenge and support to the academy management team.

5.6. IT support staff

5.6.1. Internal IT support staff are responsible for maintaining the academy's networking, IT infrastructure and hardware. IT staff will be aware of current thinking and trends in IT security and ensure that the academy system, particularly file-sharing and access to the Internet is secure. IT staff will ensure systems are not open to abuse or unauthorised external access.

5.6.2. IT support staff in academies are responsible for:

- Defending the network and infrastructure of the academy, reviewing activity logs regularly;
- Ensuring that users comply with basic access policies and that only trusted devices can connect to the academy network;
- Filtering of search facilities is robust and regularly checked for penetration to ensure that the risk of students accessing material that is unsuitable is minimised;
- To keep up to date with current threats and attack trends and take steps to mitigate this and communicate with the management team and Online Safety Co-ordinator;
- To report to the management team and Online Safety Co-ordinator on any network intrusions or other threats to the network;
- To ensure that any IT outsourced e.g. connectivity, maintenance, cloudbased services website, email provision, filtering, anti-virus, complies with DfE guidance and Data Protection regulations;
- Promoting basic cyber security practices within the academy e.g. locking computers when away from the desk, using secure passwords, caution when using USB removable drives.

5.6.3. External contractors, website designers/hosts will be made fully aware of and agree to the Trust's Online Safety Policy.

5.7. All Staff

5.7.1. Teaching and support staff are responsible for ensuring that they understand the Trust's Online Safety Policy, practices and associated procedures for reporting online safety incidents in line with academy procedures.

5.7.2. All staff will be provided with an online safety induction as part of the overall staff induction procedures. All staff will attend mandatory online safety training provided by the academy.

5.7.3. All staff will ensure that they have read, understood and signed the Acceptable Use Policy relevant to Internet and computer use in each academy.

5.7.4. All teaching staff are to be vigilant in monitoring student Internet and computer usage in line with the policy. This may include the use of personal technology, such as cameras, phones on the school site where there is a cause for concern.

5.7.5. Internet usage and suggested websites should be pre-vetted and documented in lesson planning.

5.7.6. Staff must promote and reinforce safe online practices when on and off-site, including providing advice to students on how to report incidents.

5.7.7. Staff must report as soon as is practicable any suspected misuse of Trust/academy digitally connected systems to the Headteacher or Online Safety Co-ordinator.

5.8. Designated Safeguarding Lead (DSL)

5.8.1. The DSL will be trained in specific online safety issues e.g. CEOP accredited course or equivalent.

5.8.2. The DSL will be responsible for escalating online safety incidents to the relevant external parties e.g. CEOP, local Police, Local Safeguarding Children's Board, social services and parents, and ELT. Possible scenarios might include:

- Allegations against members of staff;
- Computer crime – hacking of school systems;
- Allegations or evidence of 'grooming'; and
- Allegations or evidence of cyber bullying in the form of threats of violence, harassment or a malicious communication.

5.8.3. The DSL is responsible for acting 'in loco parentis' and liaising with websites and social media platforms, such as Twitter and Facebook, to remove instances of illegal material or cyber bullying.

5.9. Students

5.9.1. Students must ensure use of academy Internet and computer systems in agreement with the terms specified in the policy. In secondary phases, students are expected to sign the policy to indicate agreement.

5.9.2. Students are responsible for ensuring they report online safety incidents in the academy or with other external reporting facilities, such as CEOP or Childline, and are expected:

- To be aware of and comply with academy policies for Internet and mobile technology usage in the academy, including the use of personal items such as mobile phones;

- To be aware that their Internet use out of the academy on social networking sites, is covered under the Online Safety Policy if it impacts on the academy and/or its staff and students in terms of cyber bullying, reputation or illegal activities;
- To follow basic cyber security practices within the academy e.g. locking computers when away from the desk, and using secure passwords.

5.10. Parents/Carers

5.10.1. Parents/carers must support the academy in its promotion of good Internet behaviour and responsible use of IT equipment and mobile technologies both at the academy and at home.

5.10.2. Where appropriate, parents should sign the academy's Acceptable Use Policy, indicating agreement regarding their child's user and also their own use with regard to parental access to school systems such as websites, forums, social media, online reporting arrangements and questionnaires.

6. BREACH OF THIS POLICY

6.1.1. Any online safety issues should be reported to the Headteacher (academy staff) or the Director of Operations (Trust staff).

6.1.2. Any member of staff suspected of committing a breach of this Policy will be required to cooperate with an investigation. This may involve handing over relevant passwords and login details.

6.1.3. A breach of this Policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours and regardless of whether our equipment or facilities are used for the purpose of committing the breach.