LEGRA ACADEMY TRUST

E-Safety Policy

September 2023

Date created	September 2021
Version	2
Status	Ratified
Applicable to	All staff/Web
Author	ZWJ
Checked by	ALS
Valid from	September 2023
Review on	September 2024

A1. What is E-Safety?

E- Safety is often defined as 'the safe and responsible use of technology' this includes:

- The use of the internet and other means of communication
- Using electronic devices (e.g. smart phones)
- Social media
- Gaming
- Email

In the context of an inspection e- safety is described as the Academy's ability to:

- Protect and educate staff, students in their use of technology
- To have the appropriate mechanisms to intervene and support any incident where appropriate

A2. The main areas of risk of e-safety can be described in the following categories:

Content:

- Exposure to inappropriate content
- Content promoting harmful behaviours
- Hate content
- Content validation: how to check authenticity and accuracy of online content

Contact:

- Grooming (sexual exploitation, radicalisation, extremism)
- Online bullying in all forms

Conduct:

- Aggressive behaviours (bullying)
- Privacy issues, including disclosure of personal information
- Digital footprint and online reputation
- Health and wellbeing (amount of time spent online, gambling, body image)

A3. Scope of the policy:

This policy applies to all members of the Legra Academy Trust community (staff, students, volunteers, parent/carers, visitors, community users) who have access to and are users of and of the Academy ICT systems both in and outside of the academy.

A4. Roles and responsibilities:

Role	Key Responsibilities
Principal/SLT	• Has a duty of care for ensuring the safety (including e-safety of members of the Legra community. The day to day responsibility for e-safety will be delegated to the E-safety Co-ordinator and safeguarding lead. • The principal 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 (see flow on dealing with safety incidents) • Principal/Senior leaders will ensure that there is a system in place to allow for monitoring and support for all those who carry out the internal monitoring role. • SLT will receive regular monitoring reports from the E-Safety Co-ordinator • SLT to ensure that e-safety is taught embedded in the curriculum
ICT Manager and Team	• Take the day to day responsibility for e-safety issues with the safeguarding lead • Has a leading role in establishing and reviewing the academy's e-safety policies/ 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. • Reports regularly to SLT • Ensures that the academy's technical infrastructure is secure and is not open to misuse or malicious attack • Meets all the e-safety technical requirements and any Local Authority/other relevant body E-safety policy and guidance that might apply. • That users may only access the networks and devices through

Teaching and Support Staff	• Have an updated awareness of e-safety matters and the current academy e-safety policy and practices • They have read and understood and signed the Staff Acceptable Use Policy (AUP agreement) • They report any misuse or problem to Safeguarding Lead E-safety Co-ordinator for investigation / action /sanction • All digital communications with students/ parents /carers should be on a professional level and only carried out using the official Academy's systems • E- safety issues are embedded in all aspects of the curriculum and other activities • Students understand and follow the e-safety and acceptable use policies • Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright Regulations They monitor the use of digital technologies, cameras, iPads etc. in lessons and other activities. • In lessons where internet is used, sites must be checked and suitable for the students use and inform technical staff if any unsuitable material appears.
Designated Safeguarding Lead	• To deal with any of the safeguarding issues that might arise from: • Sharing of personal data • Access to illegal/ inappropriate materials • Inappropriate on-line contact with adults/ strangers • Potential or actual incidents of grooming • Cyber-bullying
Students	• Are responsible for using the academy technology systems in accordance with the student Acceptable Use Policy • Have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations. • Need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so • To know what action to take if they or someone they knows feel vulnerable when using online technology. • To understand the importance of adopting safe behaviour and good online safety practice when using digital technologies outside of the academy.
Parents/Carers	• To read, understand and promote the Academy's the Student Acceptable Use Agreement with their child where appropriate • To consult the Academy if they have any concerns about their child's use of technology • Support the academy in promoting online safety and endorse

	the parent Acceptable Use Agreement which includes the students use of photographic and video images
Community Users:	• Any external individual/organisation will sign an Acceptable Use Agreement prior to using technology Or the internet within the Academy • To model safe, responsible and positive behaviours in their own use.

A5. Education and Curriculum

Student's online safety curriculum:

This academy:

- Is currently developing a clear progressive online safety education programme as part of the Computing curriculum / PSHE. This covers a range of skills and behaviours appropriate for their age, needs and experience.
- Key e-safety messages reinforced as part of a planned programme of assemblies and tutor programme
- Students taught in all lessons to be critically aware of the materials/content they access online
- Ensure staff model safe and responsible behaviour in their own use of technology e.g. use of passwords, logging off, use of content

Education – Parents/Carers

Many parents may have only a limited understanding of e-safety risks and issues, yet they play an essential role in the education of their children and in the monitoring/regulation of their children's online behaviours. Parents may underestimate how often children and young people come across potentially harmful and inappropriate material on the internet and may be unsure about how to respond.

Belfairs Academy will therefore seek to provide information and awareness to parents and carers through:

- Newsletter
- Letters
- Academy website
- High profile events e.g. Safer Internet Day
- Parent forum
- References for helpful websites / publications
- Request online parent training via the E-safety Co-ordinator

Education Staff/volunteers/ Governors training

It is essential that all staff receive training and understand their responsibilities, as outlined in this policy.

- Training will be offered as follows:
- An e- safety audit will be carried out annually.
- A planned programme of formal e-safety training will be made available to staff.
- All new staff should receive e-safety training as part of their induction programme and fully understand the Acceptable Use Agreements.

A6. Illegal or inappropriate activities and related sanctions:

Belfairs Academy believes that the activities below are inappropriate in an academy context **(Those in bold are illegal)** and users should not engage in these activities when using academy equipment or systems **(in or outside the academy).**

Users should not visit internet sites, make post, download, data transfer, communicate or pass on material, remarks, proposals or comments that certain or relate to:

- **Child sexual abuse images (illegal- The Protection of Children Act 1978)**
- **Grooming, incitement, arrangement or facilitation of sexual acts against children (illegal- Sexual Offences Act 2003)**
- **Possession of extreme pornographic images (illegal- Criminal Justice and immigration Act 2008)**
- **Criminally racist material in Uk- to stir up religious hatred (or hatred on the grounds of sexual orientation) (illegal –Public Order Act 1986)**
- Pornography
- Promotion of any kind of discrimination
- Promotion of racialisation or extremism
- Threating behaviour, including promotion of physical violence or mental harm
- Any other information which may be offensive to colleagues or breaches the integrity of the ethos of the academy or brings the academy into disrepute.

Additionally, the following activities are also considered unacceptable on ICT equipment or infrastructure provided by the academy:

- Using the academy systems to undertake transactions pertaining to a private business
- Use systems, applications, websites or other mechanisms that bypass the filtering or other safeguards employed the academy
- Uploading, downloading or transmitting commercial software or any copyrighted materials belonging to third parties, without the necessary licensing permissions
- Revealing or publicising confidential or proprietary information (e.g. financial / personal information, databases, computer / network access codes and passwords)

- Creating or propagating computer viruses or other harmful files
- Carrying out sustained or instantaneous high volume network traffic (downloading / uploading files that causes network congestion and hinders others in their use of the internet)
- On-line gambling and non-educational gaming
- On-line shopping / commerce
- Use of social networking sites (other than in the academy's learning platform or sites otherwise permitted by the academy.

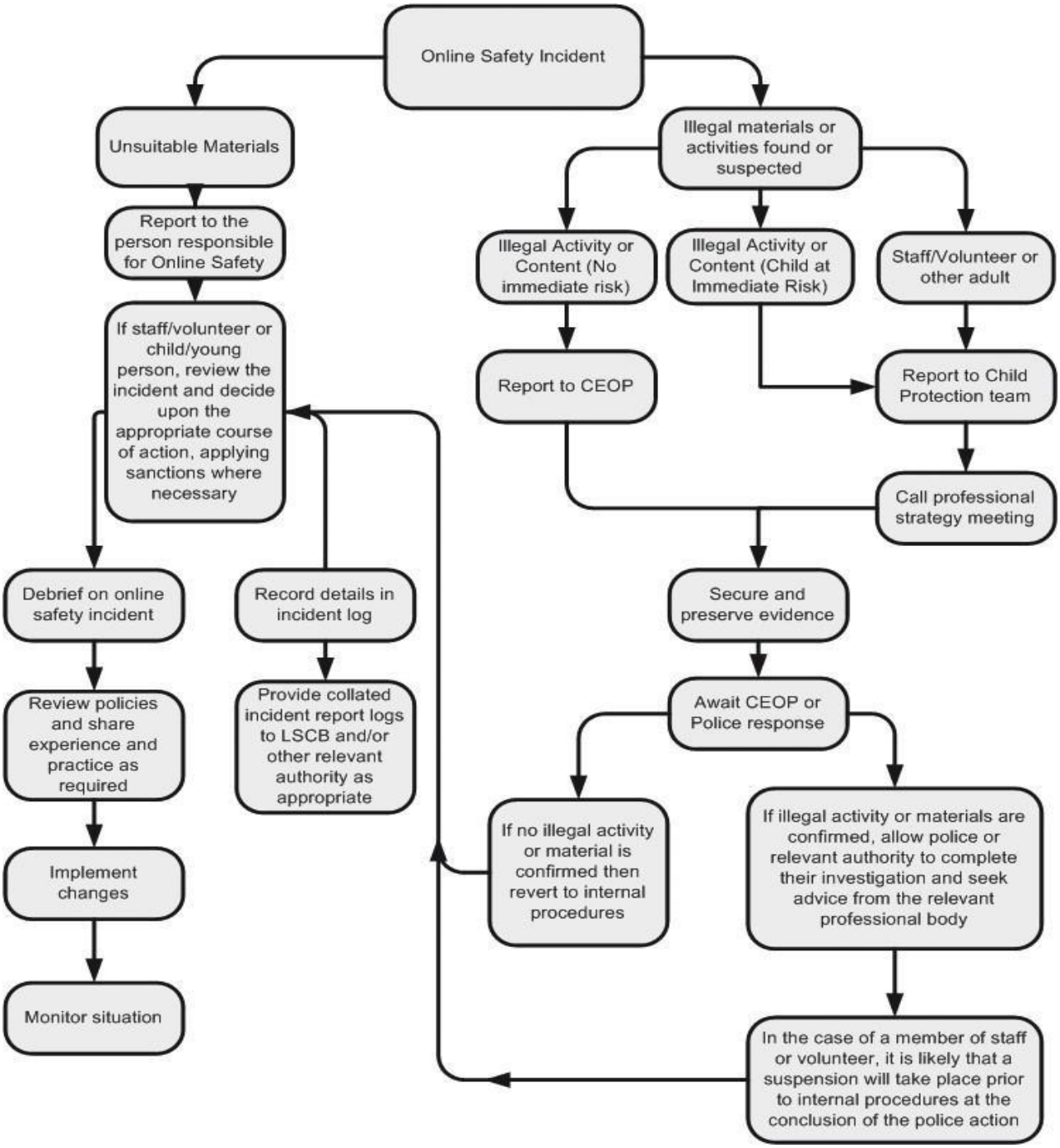
If members of staff suspect that misuse might have taken place – whether or not it is evidently illegal (see above) - it is essential that correct procedures are used to investigate, preserve evidence and protect those carrying out the investigation.

It is more likely that the academy will need to deal with incidents that involve inappropriate rather than illegal misuse. It is important that any incidents are dealt with as soon as possible in a proportionate manner, and that members of the academy are aware that incidents have been dealt with.

A7. Reporting of e-safety breaches

It is hoped that all members of the academy 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. Listed below are the responses that will be made to any apparent or actual incidents of misuse:

Particular care should be taken if any apparent or actual misuse appears to involve illegal activity listed in section 6 of this policy


Online Safety Incident
Unsuitable Materials
Illegal materials or activities found or suspected
Report to the person responsible for Online Safety
Illegal Activity or Content (No immediate risk)
Illegal Activity or Content (Child at Immediate Risk)
Staff/Volunteer or other adult
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Report to CEOP
Report to Child Protection team
Call professional strategy meeting
Debrief on online safety incident
Record details in incident log
Secure and preserve evidence
Review policies and share experience and practice as required
Provide collated incident report logs to LSCB and/or other relevant authority as appropriate
Await CEOP or Police response
Implement changes
If no illegal activity or material is confirmed then revert to internal procedures
If illegal activity or materials are confirmed, allow police or relevant authority to complete their investigation and seek advice from the relevant professional body
Monitor situation
In the case of a member of staff or volunteer, it is likely that a suspension will take place prior to internal procedures at the conclusion of the police action

A8. Professional standards for staff communication

In all aspects of their work in our academy, teachers abide by the broad **Professional Standards for Teachers** laid down by the TDA effective from September 2012:

Teachers translate these standards appropriately for all matters relating to e-safety.

Any digital communication between staff and students or parents / carers (email, chat, learning platform etc.)
must be professional in tone and content.

- These communications may only take place on official (monitored) academy systems.
- Personal email addresses, text messaging or public chat / social networking technology must not be used for these communications.

Staff constantly monitor and evaluate developing technologies, balancing risks and benefits, and consider how appropriate these are for learning and teaching. These evaluations help inform policy and develop practice.

The views and experiences of students are used to inform this process also.

Section B. Infrastructure

B.1 Password security

The academy's e-safety curriculum will include frequent discussion of issues relating to password security and staying safe in and out of academy.

B.2.1 Filtering

B.2.1a - Introduction

The filtering of internet content provides an important means of preventing users from accessing material that is illegal or is inappropriate in an educational context. The filtering system cannot, however, provide a 100% guarantee that it will do so. It is therefore important that the academy has a filtering policy to manage the associated risks and to provide preventative measures which are relevant to the situation in this academy.

B.2.1b - Responsibilities

The day-to-day responsibility for the management of the academy's filtering policy is held by the Legra ICT Manager with ultimate responsibility resting with the **CEO**. They manage the academy filtering in line with this policy and keep logs of changes to and breaches of the filtering system.

To ensure that there is a system of checks and balances and to protect those responsible, changes to the standard filtering service must be reported to, and authorised by, a second responsible person prior to changes being made (this will normally be the class teacher who originally made the request for the change).

All users have a responsibility to report immediately to class teachers / E-Safety Coordinator any infringements of the academy's filtering policy of which they become aware or any sites that are accessed, which they believe should have been filtered.

Users must not attempt to use any programs or software that might allow them to bypass the filtering/ security systems in place to prevent access to such materials.

B.2.1c - Education / training / awareness

Students are made aware of the importance of filtering systems through the academy's e-safety education programme.

Staff users will be made aware of the filtering systems through:

- signing the Acceptable Use Agreement (as part of their induction process)
- briefing in staff meetings, training days, memos etc. (timely and ongoing).

Parents will be informed of the academy's filtering policy through the Acceptable Use Agreement and through e- safety awareness sessions / newsletter etc.

B.2.1d - Changes to the filtering system

Where a member of staff requires access to a website that is blocked for use at academy, the process to unblock is as follows:

- The teacher makes the request to the network manager
- The network manager checks the website content to ensure that it is appropriate for use in the academy.

THEN
The network manager unblocks the site and logs the action in the change-control log to be reported as described above

B.2.1e - Monitoring

No filtering system can guarantee 100% protection against access to unsuitable sites. The academy will therefore monitor the activities of users on the academy network and on academy equipment.

Monitoring takes place as follows:

- Identified member(s) of staff reviews the monitoring console captures weekly
- "False positives" are identified and deleted.
- Potential issues are referred to an appropriate person depending on the nature of the capture.
- Teachers are encouraged to identify in advance any word or phrase likely to be picked up regularly through innocent use (e.g. 'goddess' is captured frequently when a class is researching or creating presentations on the Egyptians) so that the word can be allowed for the period of the topic being taught.

B.2.1f - Audit / reporting

Filter change-control logs and incident logs are made available to:

- the e-safety governor within the timeframe stated in this policy
- the LSCB on request

This filtering policy will be reviewed, with respect to the suitability of the current provision, in response to evidence provided by the audit logs.