E-Safety Policy

Aim of The Langley Academy Trust

To provide an outstanding education for every child in the trust through high aspirations and through the principles of qualify learning using curiosity, exploration and discovery.

This Policy is linked to
Child Protection Policy
Safeguarding Policy
Anti-Bullying Policy
ICT Policy

Principles

The Langley Academy Trust is committed to providing a safe and secure environment for children, staff and visitors and promoting a climate where children and adults will feel confident about sharing any concerns which they may have as a result of online safety issues.

The Langley Academy Trust recognises the need to be alert to the risks posed by strangers or others (including the parents or carers of other students) who may wish to harm children in the academy and will take all reasonable steps to lessen such risks by promotion of e-safety and acceptable use policies that are clearly understood and respected by all.

The policy is applicable to all on and off-site activities undertaken by students whilst they are the responsibility of the Trust.

Purposes

- To outline the nature of e-safety and how staff and students may identify it.
- To identify simple ways in which e-safety can be reported to responsible adults.
- To provide a clear policy and guidelines to enable e-safety to be tackled effectively.
- The E-Safety lead in each Academy will be the Designated Child Protection Officer.

Guidelines

Why the Internet and digital communications are important

- The Internet is an essential element in 21st century life for education, business and social interaction. The school has a duty to provide pupils with high-quality Internet access as part of their learning experience.
- Internet use is a part of the statutory curriculum and a necessary learning tool for staff and students.

Internet use will enhance and extend learning

- Staff will be made aware of and students will be educated in the safe use of the internet
- Clear boundaries will be set and discussed with staff and students, for the appropriate use of the Internet and digital communications.
- Students will be educated in the effective use of the Internet in research, including the skills of knowledge location, retrieval and evaluation.

Students will be taught how to evaluate Internet content

- Schools should ensure that the use of Internet derived materials by staff and by students complies with copyright law
- Students should be taught to be critically aware of the materials they read and shown how to validate information before accepting its accuracy

Managing Internet Access

Information system security

- The Trust's ICT system security will be reviewed regularly.
- Virus protection will be installed and updated regularly.

E-mail

- Students and staff should only use approved curriculum e-mail accounts.
- Students must be made aware of how they can report abuse and who they should report abuse to.
- Students must report any offensive or inappropriate e-mail they receive to a member of staff.
- In e-mail communication, students must not reveal their personal details or those of others, or arrange to meet anyone without specific permission.
- Incoming e-mail should be treated as suspicious and attachments not opened unless the author is known.
- The Trust should consider recommending a standard mail format for all users.
- The forwarding of chain letters is not permitted.
- Staff must use the school E-mail account for communicating electronically regarding school business.
- The use of Academy E-Mail is solely for professional use.
- Staff must follow additional steps to ensure sensitive data is secure when sending information via E-mail.

Published content and the school web site

- Staff or student personal contact information will not generally be published. The contact details given online should be the school office.
- The Executive Principal or nominee will take overall editorial responsibility and ensure that published content is accurate and appropriate.

Published content and the Academy VLE

- Staff or student private and personal contact information will not generally be published. The contact details provided will be the person's official curriculum e-mail address

Publishing students' images and work

- Photographs that include students will be selected carefully so that images of individual students cannot be misused.

- Students' full names will not be used anywhere on the Trust Web sites or other on-line space, particularly in association with photographs.
- Written permission, using the approved permission form, from parents or carers will be obtained before photographs of students are published on the Trust Web sites/VLE.
- Work can only be published with the permission of the pupil and parents/carers.

Social networking and personal publishing

The Trust will educate people in the safe use of social networking sites, and educate students in their safe use. Students will be advised never to give out personal details of any kind which may identify them, their friends or their location.

- Students must be made aware of how they can report abuse and who they should report abuse to.
- Students should be taught the reasons why personal photos should not be posted on any social network space without considering how the photo could be used now or in the future.
- Students should be advised on security and encouraged to set passwords, to deny access to unknown individuals and to block unwanted communications. Students should only invite known friends and deny access to others.
- Staff are advised not to run social network spaces for student use on a personal basis.
- Staff will be advised not to include work related contacts (parents, pupils or ex-pupils) on their social network space.
- The discussion of work related matters/information by staff, on a social network site is forbidden and would become a disciplinary matter for those who breached this principle.
- Staff may not upload school images of pupils onto their social network site, and would become a disciplinary matter for those who breached this principle.
- Staff must be aware that information stored, displayed or discussed on social networking sites are in the public domain.
- Parents, pupils and staff should be aware that bullying can take place through social networking sites. (see section below)

Managing monitoring and filtering

- Senior staff will ensure that regular checks are made to ensure that the filtering methods selected are appropriate, effective and reasonable.
- If staff or pupils discover an unsuitable site, it must be reported to the E-Safety Lead or the Network Manager.
- Logs of internet breeches are kept and reviewed. Access to any illegal, suspicious websites will be reported to the appropriate agencies.

Managing videoconferencing

- Students should ask permission from the supervising teacher before making or answering a videoconference call.
- Videoconferencing will be appropriately supervised for the students' age.
- Primary schools will seek permission from parents and guardians before children can take part in videoconferences.

- Staff will establish dialogue with other conference participants to make an assessment of the risk, before taking part in a videoconference. If it is a non-school site it is important to check that they are delivering material suitable for the class.

Managing emerging technologies

- Emerging technologies will be examined for educational benefit and a risk assessment will be carried out before use in school is allowed.
- The Directorate and senior leaders are aware that technologies such as mobile phones with wireless Internet access can bypass school filtering systems and present a new route to undesirable material and communications.
- Where contact with Students is required to facilitate their learning, staff will be issued with a school phone.
- The sending of abusive or inappropriate text messages is forbidden.
- The use by students of cameras in mobile phones will be kept under review.
- In primary schools the use of mobile phones during lessons or formal school time is forbidden
- It should be noted that games machines including the Sony Playstation, Microsoft Xbox and others have Internet access which may not include filtering. Care is required in any use in the Academy or other officially sanctioned location.

Protecting personal data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 1998.

- Data that contains sensitive information, be it personal information or work related information (eg documents about pupils) needs to be encrypted to ensure its safety. This applies whether data is on a hard drive or portable storage device.
- Users must securely delete personal or sensitive data when it is no longer required.
- Any personal or financial data transferred electronically should be encrypted or password protected.

Policy Decisions

Authorising Internet access

- All staff and visitors must read and sign the 'Staff Acceptable Use Policy and Code of Conduct for ICT' before using any school ICT resource, including any laptop issued for professional use.
- The Trust will maintain a current record of all staff and students who are granted access to school ICT systems.
- Secondary age students must apply for Internet access individually by agreeing to comply with the Responsible Internet Use statement contained within the Academy's Acceptable User policy.
- Parents/carers will be asked to sign and return a consent form.

Assessing risks

Handling e-safety complaints

- Complaints of Internet misuse will be reported to the e-safety Lead.
- Any staff misuse that suggests a crime has been committed, a child has been harmed or that

a member of staff is unsuitable to work with children should be reported to the LADO within one working day in accordance with Slough Safeguarding Board policies.

- Any complaint about staff misuse must be referred to the Executive Principal and if the misuse is by the Executive Principal / Headteacher it must be referred to the chair of governors in line with the Trust's Safeguarding and Child Protection procedures.
- Students, parents and staff will be informed of the complaints procedure.

The Trust will take all reasonable precautions to prevent access to inappropriate material. However, due to the international scale and linked nature of Internet content, it is not possible to guarantee that unsuitable material will never appear on a computer connected to the Trust network. The Trust cannot accept liability for any material accessed, or any consequences of Internet access.

The Trust should audit ICT use to establish if the E-Safety policy is adequate and that the implementation of the E-Safety policy is appropriate and effective. The Trust will ensure monitoring software and appropriate procedures are in place.

Communicating E-Safety

Introducing the E-safety policy to students

E-Safety rules will be posted in all rooms where computers are used All system users will be informed that network and Internet use will be monitored.

- A programme of E-Safety training and awareness raising will be put in place as part of the pastoral programme.
- In primaries, an e-safety module will be included throughout the curriculum, particularly in PSHE and Computing programmes of study, covering both school and home use.

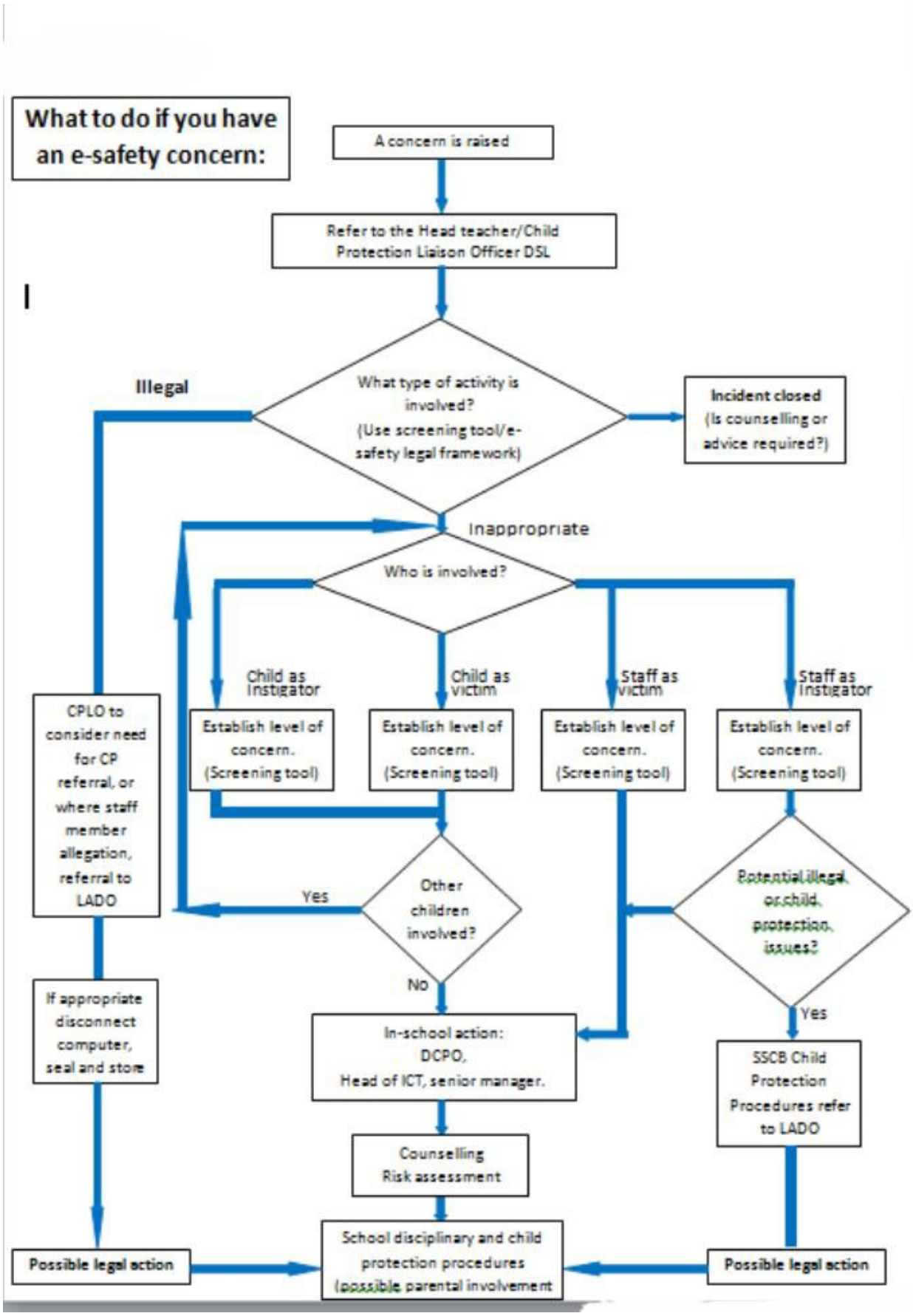
Staff and the E-Safety policy

- All staff will be given access to the Trust's E-Safety Policy and its importance explained. Staff must be informed that network and Internet traffic can be monitored and traced to the individual user, including staff laptops.
- Staff that manage filtering systems or monitor ICT use will be supervised by senior leadership and work to clear procedures for reporting issues.
- Staff should understand that phone or online communications with students can occasionally lead to misunderstandings or even malicious accusations. Staff must take care always to maintain a professional relationship.
- Staff training in safe and responsible Internet use and on the school E-safety Policy will be provided as required.

Enlisting parents' and carers' support

- Parents' and carers' attention will be drawn to the Trust's E-Safety Policy in newsletters and on the Trust's website and the VLE site.
- The Trust will maintain a list of E-safety resources for parents/carers.

Review Date: November 16
Ratified Date: November 16
Author: Alison Lusuardi
Date of next review: November 17


What to do if you have an e-safety concern:
A concern is raised
Refer to the Head teacher/Child Protection Liaison Officer DSL
What type of activity is involved? (Use screening tool/e-safety legal framework)
Illegal
Incident closed (Is counselling or advice required?)
Inappropriate
Who is involved?
Child as Instigator
Child as victim
Staff as victim
Staff as Instigator
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
Establish level of concern. (Screening tool)
CPLO to consider need for CP referral, or where staff member allegation, referral to LADO
Other children involved?
Yes
No
Potential illegal or child protection issues?
Yes
If appropriate disconnect computer, seal and store
In-school action: DCPO, Head of ICT, senior manager.
SSCB Child Protection Procedures refer to LADO
Counselling Risk assessment
Possible legal action
School disciplinary and child protection procedures (possible parental involvement
Possible legal action