E-Safety Policy

Document control	
Document title	E-Safety Policy
Document status	Approved at Education Committee
Author	Mrs Claire Gilding-Brant
Effective date	August 2023
Version	V.6
Date of next review	January 2025
Location	Website/OneNote/Network

Version	Author	Date	Changes
V.5	CGB	August 2023	Section 4 Filtering & Monitoring
V6	CGB	Jan 2024	DSL responsibility for e-safety, KCSiE & Prevent Duty as a result of Prevent Risk Assessment

CONTENTS

1. Scope

This guidance is applicable to all those involved in the provision of e-based education/resources at the school and those with access to / are users of school IT systems.

2. Objectives

- To ensure that pupils are appropriately supervised during school activities.
- To promote responsible behaviour with regard to e-based activities.
- To take account of legislative guidance, in particular KCSiE (inc. Filtering & Monitoring, 2023), The Prevent Duty, the General Data Protection Regulations and the Data Protection Act 2018.

3. Guidance

The DSL will act as E-Safety Co-ordinator and will:

- ensure that all staff are aware of this guidance
- compile logs of e-safety incidents
- liaise with School technical staff
- provide / arrange for staff training
- liaise with the Head on any investigation and action in relation to e-incidents
- advise on e-safety policy review and development.

The Head of Digital Strategy will:

- be responsible for the IT infrastructure and ensure it is not open to misuse or malicious attack
- ensure that users may only access the networks and devices through an enforced password protection policy
- keep up to date with e-safety technical information
- ensure that the use of the network (including Internet, virtual learning, email and remote access) is monitored for misuse
- implement any agreed monitoring software / systems
- liaise with external service providers who fully manage our firewalls and servers.

Teaching and Support Staff will:

- maintain awareness of School e-safety policies, procedures and practices
- report any suspected misuse or problem to the Head or E-Safety Co-ordinator
- ensure that digital communications with all members of the School community are professional and conducted *via* School systems
- ensure e-safety is recognised, where appropriate, in teaching activities and curriculum delivery
- ensure pupils understand and follow e-safety procedures, including avoiding plagiarism and upholding copyright regulations
- monitor the use of digital technologies (including mobile devices, cameras etc) during School activities
- ensure that where the use of the Internet is pre-planned, pupils are guided to sites checked as suitable for their use and that procedures are in place for dealing with any unsuitable material that is found in searches.

Pupils will:

- be responsible for using School systems in accordance with the Acceptable Use policy
- understand and follow e-safety procedures, including avoiding plagiarism and upholding copyright regulations

- understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- be expected to know the policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying
- understand that the e-safety policy will include actions outside of School where related to School activities.

Parents/Guardians will:

- be advised of e-safety policies through parents' evenings, newsletters, letters, the website etc.
- be encouraged to support the School in the promotion of good e-safety practice
- follow School guidelines on:

a. digital and video images taken at School events
b. access to parents' sections of the School website / pupil records
c. the use of their children's personal devices in the School (where this is permitted).

Child Protection

Those responsible should be trained in e-safety and aware of the implications that may arise from:

- sharing personal data
- access to illegal / inappropriate materials including nudes and semi-nudes
- inappropriate contact with other users on-line
- potential or actual incidents of grooming
- cyber-bullying.

Community Users/Contractors.

Where such groups have access to School networks / devices, they will be expected to provide signed acceptance to abide by School e-safety policies and procedures.

4. **Filtering and Monitoring**

School has identified and assigned the roles and responsibilities for managing Filtering and Monitoring systems. The DSL is the E safety co-ordinator and works closely with the Director of Information Systems (DIS) to implement the safe and effective use of all E systems in school.

If there is an attempt to access potentially harmful and inappropriate content the following procedure is followed.

- The IT services Team receives an initial notification immediately upon an attempt to access content which could be deemed harmful. This is managed via SOPHOS software
- The team will complete an immediate high-level review
- If there is a serious indication of possible harm the DIS is informed and classifies the severity of the notification.
- The DIS is a member of the Extended Leadershsip Team and will escalate to the DSL if necessary and raise on My Concern.
- The IT team will go straight to the DSL if the DIS is not available

Any concern about the child will be followed up using the processes outlined in the School's Child Protection Policy.

In addition to the above procedure the DSL meets regularly with the DIS to review the Schools Filtering and Monitoring systems. Agenda items include:-

1. Staff training – device management
2. E safety calendar– parents/pupils
3. Points of note
4. Areas of concern
5. Overview of weekly firewall reports
6. SOPHOS central report

As part of the annual safeguarding report to Governors, Filtering and Monitoring is explained and commented on.

School ensures that any harmful and inappropriate content is blocked without unreasonably impacting the high standards of teaching and learning. Staff and students can request a site to be opened on review of IT services team, DSL and DIS.

School has highly effective monitoring strategies in place that meet the children's safeguarding needs. Thes includes Firewalls, Network (AD), Microsoft 365 and Impero.

School has a duty to limit the exposure of potentially harmful and inappropriate online material. Staff training will include online safety which amongst other things will include and understanding of the expectation, applicable roles and responsibilities in relation to Filtering and Monitoring during induction which will include the school network and devices.

Regular INSET will be provided for staff which includes termly INSET, external speakers, courses on EDUCARE, Teach Meet programmes and internal staff expertise. All members of the School community can also request support through the LHS Help Desk email, helpdesk@luckleyhouseschool.org.