Luckley HOUSE SCHOOL

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 2024
Location	Website/OneNote/Network

Version	Author	Date	Changes
V.5	CGB	August 2023	No changes
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, 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.

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.