HATHEROP CASTLE
PREP SCHOOL & NURSERY

E-Safety Policy

Reference:	B04
Version number:	1.1
Last updated:	September 2022
Date of next review:	September 2023 or if legislation/statutory requirements change

Summary of changes and reviews

Version	Date	Summary of amendments	By
1.0	20 Mar 20	Version control numbering implemented. Updated to include adoption to Censornet.	SB
1.1	Sept 2022	Reviewed and updated where appropriate	NR

Contents

E-SAFETY POLICY

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 ICT systems.

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 the General Data Protection Regulations and the Data Protection Act 2018.

Guidance

The School Business Manager is responsible for the implementation of this policy. Responsibilities are outlined below:

The School Business Manager

The School Business Manager will:

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

The Group IT Manager

The Wishford Group IT Manager will:

- be responsible for the IT infrastructure and ensure that 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 in order to carry out their role;
- ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse where deemed necessary; and
- implement monitoring policies on Censornet.

Teaching and Support Staff

Teaching and support staff will:

- maintain awareness of school e-safety policies and practices;
- report any suspected misuse or problem to the Head Teacher or Head of Digital Learning;
- ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;
- where relevant e-safety is recognised in teaching activities and curriculum delivery;
- ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;

- monitor the use of digital technologies (including mobile devices, cameras etc during school activities); and
- ensure that where the use of the internet is pre-planned, pupils are guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found in internet searches.

Child Protection

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

- sharing of personal data;
- access to illegal / inappropriate materials;
- inappropriate contact on-line with adults / strangers;
- potential or actual incidents of grooming; and
- cyber-bullying.

Pupils

Pupils:

- are responsible for using school digital technology systems in accordance with the school's IT Acceptable Use Policy (B01);
- will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;
- will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;
- are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying; and
- will understand that the e-safety policy will include actions outside of school where related to school activities.

Parents/Carers

Parents/carers:

- will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc;
- will be encouraged to support the school in the promotion of good e-safety practice; and
- should follow school guidelines on:
- digital and video images taken at school events;
- access to parents' sections of the school website / pupil records; and
- their children's / pupils' personal devices in the school (where this is permitted).

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.

Legal Requirements & Education Standards

References are as follows:

- Commentary on the Regulatory Requirements September 2018, Part 3 (www.isi.net).
- Reference Guide to the key standards in each type of social care service inspected by OFSTED (www.ofsted.gov.uk).
- Health and Safety at Work" Section H of the ISBA Model Staff Handbook.

- “Health and Safety and Welfare at Work” Chapter N of the ISBA Bursar’s Guide.
- “Insurance” Chapter K of the Bursar’s Guide by HSBC Insurance Brokers Ltd.
- UK Council for Child Internet Safety (www.edcuation.gov.uk/ukccis).
- Cyber-bullying.org (www.cyberbullying.org).
- Department for Education "Safer Working Practice for Adults who Work with Children and Young People" (www.education.gov.uk).
- DfE Data Protection: a toolkit for schools.