E-Safety Policy

Independent Day School for Boys and Girls

Fairley House School

1st September 2019

Date:	September 2019
Date for update/review:	September 2020
Named person responsible for review:	ICT Coordinator
Approved by:	Headmaster

E-Safety Policy

1.1 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 ICT systems.

1.2 Objectives

1.2.1 To ensure that pupils are appropriately supervised during school activities.

1.2.2 To promote responsible behaviour with regard to e-based activities.

1.2.3 To take account of legislative guidance, in particular the General Data Protection Regulations and the Data Protection Act 2018.

1.3 Guidance

1.3.1 The IT Manager will be responsible for the implementation of this policy.

1.3.2 The IT Manager will act as E- Safety Co-ordinator and will:

(a) compile logs of e-safety incidents;

(b) report to the Head Teacher on recorded incidents;

(c) ensure that staff are aware of this guidance;

(d) provide / arrange for staff training;

(e) liaise with school technical staff;

(f) liaise with the Head Teacher on any investigation and action in relation to e-incidents;

(g) advise on e-safety policy review and development.

1.3.3 The School ICT Co-ordinator and IT Department will:

(a) be responsible for the IT infrastructure and that it is not open to misuse or malicious attack;

(b) ensure that users may only access the networks and devices through an enforced password protection policy;

(c) keep up to date with e-safety technical information in order to carry out their role;

(d) ensure that the use of the network (including internet, virtual learning, email and remote access) is monitored for misuse;

(e) implement any agreed monitoring software / systems.

1.3.4 Teaching and Support Staff will:

(a) maintain awareness of school e-safety policies and practices;

(b) report any suspected misuse or problem to the Head Teacher or E-Safety Co-ordinator;

(c) ensure that all digital communications with pupils / parents / carers/ fellow staff are on a professional level and conducted on school systems;

(d) where relevant e-safety is recognised in teaching activities and curriculum delivery;

(e) ensure pupils understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;

(f) monitor the use of digital technologies (including mobile devices, cameras etc during school activities;

(g) 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.

1.3.5 Child Protection

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

(i) sharing of personal data;

(ii) access to illegal / inappropriate materials;

(iii) inappropriate contact on-line with adults / strangers;

(iv) potential or actual incidents of grooming; and

(v) cyber-bullying.

1.3.6 Pupils

(a) are responsible for using school digital technology systems in accordance with the school acceptable use policy;

(b) will understand and follow e-safety policies, including the need to avoid plagiarism and uphold copyright regulations;

(c) will understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so;

(d) are expected to understand policies on the use of mobile devices and digital cameras, the taking / using of images and cyber-bullying;

(e) will understand that the e-safety policy will include actions outside of school where related to school activities.

1.3.7 Parents / Carers

(a) will be advised of e-safety policies through parents' evenings, newsletters, letters, school website etc;

(b) will be encouraged to support the school in the promotion of good e-safety practice; and

(c) should follow school guidelines on:

(i) digital and video images taken at school events;

(ii) access to parents' sections of the school website / pupil records;

(iii) their children's / pupils' personal devices in the school (where this is permitted).

1.3.8 Community Users / Contractors

(a) 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.