PROSPECT HOUSE

SCHOOL

DIGITAL USAGE POLICY

INCLUDING e-SAFETY

SEPTEMBER 2023

(text marked in blue refers to the Data Protection Policy or to data protection considerations)

ACCEPTABLE USAGE POLICY – PUPILS

I promise to use the school ICT only for schoolwork that a teacher has asked me to do.

I promise not to look for or show other people things that may be upsetting.

I promise to show respect for the work that other people have done.

I will not use other people's work or pictures without permission to do so.

I will not damage the ICT equipment. If I accidentally damage something I will tell a teacher.

I will not share my password with anybody. If I forget my password I will let my computing teacher know.

I will not use other people's usernames or passwords.

I will not share personal information online with anyone.

I will not download anything from the Internet unless a teacher has asked me to.

I will let a teacher know if anybody asks me for personal information.

I will let a teacher know if anybody says or does anything to me that is hurtful or upsets me.

I will be respectful to everybody online.

I will treat everybody the way that I want to be treated.

I understand that some people on the Internet are not who they say they are, and some people can be nasty. I will tell a teacher if I am ever concerned in school, or tell my parents if I am at home.

I understand if I break the rules in this acceptable usage policy there will be consequences and my parents will be told.

ACCEPTABLE USAGE POLICY – STAFF

Internet access – Staff must not visit Internet sites, make, post, download, upload, data transfer, communicate or pass on, material, remarks, proposals or comments that contain or relate to: child abuse; pornography; discrimination of any kind; the promotion of racial or religious hatred; the promotion of illegal acts; statements or images that are intended to radicalise people or in any other way endorse, condone or incite extremist or terrorist activities; contain threatening behaviour, including promotion of physical violence or mental harm; any information which breaches the integrity of the ethos of the school or brings the school into disrepute or any other information which may be illegal or offensive.

Inadvertent Internet access must be treated as an e-safety incident, reported in writing to the e-safety officer.

Social networking – This is allowed in school in accordance with the Digital Usage Policy only and as outlined in the Staff Code of Conduct within the Safeguarding Policy. Staff using social networking for personal use should never undermine the school, its staff, parents or children. Staff must not become "friends" with parents or pupils or former pupils on personal social networks such as Facebook, Twitter, Instagram or LinkedIn.

Use of Email – Staff are not permitted to use school email addresses for personal correspondence unrelated to school business. All email should be kept professional: whilst there can be no objection to a degree of informality in internal emails, the body text of any intended to go outside the school, for example to parents, should be composed no less rigorously than an old-fashioned letter. Staff are reminded that school data, including emails, is open to subject access requests under the DPA 2018.

Passwords - Staff should keep passwords private and never save these on school devices. There is no occasion when a password needs to be shared with another member of staff, pupil or IT support.

Data Protection – If it is necessary for staff to take work home, or offsite, they should ensure that any devices they intend to use are encrypted. On no occasion should data concerning personal information be taken offsite on an unencrypted device.

Personal Use of School ICT - Staff are not permitted to use ICT equipment for personal use unless specific permission has been given from the Head, who will set the boundaries of personal use.

Images and Videos - Staff must not without consent upload on to any Internet site or service images or videos of themselves, other staff or pupils. This is applicable not only professionally (in school) but also personally (e.g., staff social events).

Use of Personal ICT - use of personal ICT equipment is not to be used except at the discretion of the Head and the Head of computing.

Viruses and other malware - any virus outbreaks must be reported to the e-safety officer who will advise the Head and the Technical Support team as soon as is practicable to do so, along with the name of the virus (if known) and actions taken by the school.

Social Media - e-safety – like health and safety, e-safety is the responsibility of everyone. As such staff will promote positive e-safety messages in all use of ICT whether they are with other members of staff or with pupils.

Any member of staff who suspects that a member of the school community is accessing inappropriate material or is not abiding by the school's e-safety policy and protocols must report any allegation, complaint, concern or suspicion directly to the Head. If the Head is absent or if the Head is the subject of the concern, the concern must be reported to the Governor of the school.