

ACCEPTABLE USE POLICY (STAFF)

This section should be completed following ratification of the Policy.

Audience	All Staff, Trustees and volunteers
Ratified	September 2026
Other Related Policies	Code of conduct & General Data Protection Policy, Online Safety Policy & Child Protection & Safeguarding Policy
Policy Owner	Trust Safeguarding Team & ARC Committee
Review Frequency	Within 18 months

Ownership

Preston Hedges Trust is responsible for the production and maintenance of this document. It is issued by the Clerk, clerk@prestonhedges.org to whom any change requests or queries should be directed.

Acceptable Use Policy – Staff

You must read this policy in conjunction with the Online Safety Policy. Once you have read and understood both, you must sign that you have read and agreed to the Acceptable Use Policy. This policy forms part of the terms and conditions set out in your contract of employment.

Internet access – You must not access or attempt to access any sites that contain any of the following: child abuse; pornography; promoting discrimination of any kind; promoting racial or religious hatred; promoting illegal acts; any other information which may be illegal or offensive to colleagues. Inadvertent access must be treated as an online safety incident, reported to the Online Safety officer and an incident sheet completed. Any incidents may result in disciplinary action and may need to be reported to the Police.

Social networking – Staff using social networking for personal use should never undermine the Trust, the school, its staff, parents or children. Staff should not seek to become “friends” with parents or pupils on personal social networks. It is understood that there may be existing relationships of staff living on an estate, but these must be open & disclosed to the Principal or COO and the DSL.

Use of Email – staff are not permitted to use school email addresses for personal business. All emails should be kept professional. Staff are reminded that school data, including emails, is open to Subject Access Requests under the Freedom of Information Act.

Passwords – Staff should keep passwords private.

Data Protection – If it is necessary for you to take work home, or off site, you should ensure that this is through a password protected USB or encrypted and password protected laptop.

Personal Use of School ICT – You are not permitted to use ICT equipment for personal use unless specific permission has been given from the Principal or COO who will set the boundaries of personal use. Permission must be sought stating the reason for using personal equipment; a risk assessment will be carried out by IT support and the Online Safety Officer or COO.

Images and Videos – You should not upload onto any internet site or service images or videos of other staff or pupils without consent. This is applicable professionally (in school) or personally (i.e. staff outings). The Trust and schools must be supported

in its approach to online safety and staff must not deliberately upload any images or videos that could upset a member of the school community

Professional Role –Staff should ensure that all online activity, inside and outside school, will not bring themselves, colleagues, the Trust or school into disrepute.

Mobile Phones – Staff must ensure that mobile phones are never used in class to answer calls or respond to messages. They should be kept out of sight of the children and not be visible in the classroom with children. Taking photographs on personal devices is prohibited at school. To safeguard yourself, mobile phones should be left in the classroom cupboard or staffroom during the school day and checked away from the children in either the cupboard, offices or staffroom.

Viruses and other malware - any virus outbreaks are to be reported to IT support as soon as it is practical to do so, along with the name of the virus (if known).

Online Safety – like health and safety, online Safety is the responsibility of everyone. As such you will promote positive online safety messages in all use of ICT whether you are with other members of staff or with students.

Note – All users are reminded that Internet will be monitored without prior notice. This is to ensure, as much as possible, that users are not exposed to illegal or inappropriate websites, and to ensure, as much as possible, that users do not actively seek access to illegal or inappropriate websites.

ONLINE SAFETY / ACCEPTABLE USE POLICY

I have read and agree to adhere to the terms of the Acceptable Use Policy

[illegible]