

Acceptable Use & E Safety Guidance for Staff

Effective from: September 2025

Authorised by: Mary Fysh; Principal, Sarah Tapp; Head and Martin Ayres; Chair of Advisory Body

NB To be read in conjunction with the school's Child Protection and Safeguarding Policy and requirements for the use of mobile phones and cameras as set out within the EYFS framework and other school policies.

INTERNET ACCESS

You must not access, or attempt to access, websites 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 or children

It is recognised that under certain circumstances inadvertent access may happen. Should you or a student access any of these sites unintentionally you should report the matter immediately to the Principal or Head so that it can be logged.

INAPPROPRIATE / ILLEGAL CONTENT

Access to any of the following will be reported to the Police:

- images of any form of sexual abuse, including child sexual abuse (sometimes incorrectly referred to as child pornography). These are
- images of children apparently under 16 years old involved in sexual activity or posed to be sexually provocative
- adult material that potentially breaches the Obscene Publications Act;
- Any material deemed to be criminally racist in the UK.

SOCIAL NETWORKS

Members of staff should never knowingly become "friends" with children on any social networking site or engage with children on internet chat.

COMMUNICATION

All members of staff should use their school email address or Scholar Pack communications for conducting professional business. This includes communicating with parents and students.

REMOTE ACCESS

Staff are permitted to access their school documents. Please ensure full compliance with data protection and do not leave your home computer unattended when logged in.

PASSWORDS

Keep your passwords private. Passwords are confidential and personal. On no account should a member of staff allow another person to use their staff login.

DATA PROTECTION

Where a member of staff has to take home sensitive or confidential information, sufficient safeguards should be in place to prevent loss or misuse, i.e. is it really necessary to take it all home, can it be encrypted and does it have to be on a USB memory stick that can be easily misplaced? All data relating to staff, students and parents must be kept private and confidential.

PERSONAL USE

Staff are not permitted to use ICT equipment for personal use without the Principal or Heads approval. If personal use is permitted the boundaries of use will be written down and staff are expected to adhere to the written requirements. Misuse of school computers will be regarded as a disciplinary matter.

IMAGES AND VIDEOS

No images or videos should ever be uploaded to a website or social network without the express permission of parents or the child's carer. Similarly no personal information (name, date/place of birth, mobile number, email address etc.) should ever be shared.

STORAGE OF SCHOOL DEVICES

All school devices must be kept stored in a cupboard or drawer when not in use and not left unattended and accessible to any other personnel or visitors.

USE OF PERSONAL ICT DEVICES / Bring Your Own Devices (BYOD)

Use of personal ICT equipment (i.e. mobile phones, cameras, personal laptop etc.) is at the discretion of the Principal or Head. Any such use should be strictly checked for up to date anti-virus and malware checkers. Use of personal ICT devices is subject to the same Acceptable Use Policy. Pictures or videos of children must **never** be taken using personal ICT devices.

REPORTING CONCERNS

It is the duty of staff to support the school's Child Protection/Safeguarding policy and report any behaviour (staff or students), which is inappropriate or a cause for concern, to the Principal or Head.

MONITORING

Emails and internet activity are subject to routine and random monitoring.