| E Safety and Social Media Use Policy | | | |
|---|---|---|---|
| **Version 5** | | | |
| **Approval date** | 07.10.25 | **Approved by** | LGB |
| **Next Review Date** | October 2027 | **Lead Reviewer** | TLR Technology |

## Introduction and aims

ICT (Information and Communication Technology), including data, and the related technologies such as e-mail, the Internet and mobile devices (such as laptop computers and iPads) are an expected part of our daily working life in school. This policy is designed to ensure that all staff (including agency staff, volunteers, students on placement and Governors) are aware of their professional responsibilities when using any form of ICT. It is also designed to make it clear to staff and parents what is expected of pupils in terms of safe use of technology.

## Implementation

### Use of the School Network

- All Internet activity during school time should be appropriate to staff's professional activity or the pupil's education;
- Pupil data including personal information, assessments and photos should only be processed and stored on approved school equipment apps and software;
- Staff should always ensure that personal and organisational data is NOT used when working with AI tools. They must verify that tools meet data security standards before using them for work related to the school.
- Staff must only use AI technologies approved by the school for work purposes. Any accounts should be configured to comply with organisational security and oversight requirements, reducing the risk of data breaches.
- All Internet activity is filtered and monitored by Smoothwall;
- All Internet activity by pupils should be supervised by staff;
- Internet activity that threatens the integrity or security of the school's ICT systems, or activity that attacks, corrupts, or threatens the security of other organisations' systems, is prohibited;
- The Schools Network and associated equipment will not be used to access, display, store, transmit, distribute, edit or record inappropriate sites such as those containing pornographic, violent, racist, discriminatory, criminal skills related, illegal drugs related or offensive material;
- The Network must not be used to download entertainment software or games;
- Uploading materials or files to MAT (Multi Academy Trust) systems must only be performed on machines that have virus protection to the latest Corporate Standards;
- Downloading of files to school systems using ftp, e-mail and http must be carried out with an appropriate level of care and thought. Problems arising from the installation of files, utilities and software updates obtained by such methods are the school's responsibility. Virus infection caused by such methods on machines without protection to the latest Corporate Standards will be the employee's responsibility;

- The Network must not be used to engage in any activity for personal gain or personal business transactions;
- The Network must not be used to conduct or host any on-going non-Education related activities, including discussion groups, chat lines, newsgroups or any other form of on-line club;
- The Network must not be used for personal or commercial advertisements, solicitations or promotions;
- Pupils found to be accessing unsuitable online material will have their access to certain websites restricted or in certain cases lose all access to the Internet and may be subject to school disciplinary procedures;
- Staff found to be accessing unsuitable online material will be subject to school disciplinary procedures.

**Email Use**

- Access to e-mail should only be made via the authorised account and password, which must not be made available to any other person;
- Users must not pretend that they are someone else when sending e-mail, for example, by using someone else's account to send a message;
- Staff are expected to use email in a professional, respectful, and courteous manner at all times. Language should be clear, constructive, and aligned with the values of the Specialist Schools Trust and Great Oaks School;
- To support staff wellbeing and work–life balance, emails should ordinarily be sent between 6:00am and 6:00pm. Staff are encouraged to avoid sending non-urgent emails outside of these hours unless there are exceptional circumstances;
- When communicating with colleagues via email or other electronic platforms, staff must demonstrate the same standards of professionalism as they would in face-to-face interactions. Disrespectful, dismissive, or inappropriate communication is not acceptable;
- As e-mail can be forwarded or inadvertently sent to the wrong person, the same professional levels of language and content should be applied as for letters or other media;
- Changes must not be made to other people's messages which are then sent on to others without making it clear where the changes have been made;
- Messages that contain abusive language, extreme viewpoints, that libel others, or that infringe the privacy rights of others are forbidden;
- Staff members are responsible for ensuring that any e-mail sent or resulting contacts made outside of the organisation do not bring the school into disrepute;
- Posting anonymous messages and creating or forwarding chain letters is forbidden;
- Users must not publish, electronically or otherwise, any school e-mail address as a point of contact for non-educational related activities;
- Personal or otherwise sensitive data should not be transferred via e-mail unless the security of the data whilst in transit can be assured.

**Staff Use of Social Networking Sites**

- The school has an expectation that any use of social networking sites (e.g. Facebook, Twitter, Instagram, Snapchat) by staff does not bring the name of the school, or any of its staff or pupils into disrepute;
- All staff are advised to set security and privacy filters to a maximum on such social networking sites to avoid making private details public;

- Staff should never give personal contact details to students or their families and maintain clear professional boundaries online
- Staff should NOT accept contact from pupils or parents via social networking sites under any circumstances;
- Staff should NOT use Social Media to discuss any school-related business with other professionals.
- If pupils do attempt to make contact with staff via social networking sites it should be reported to a member of LMT as soon as possible;
- Photographs featuring pupils should NOT be published on social networking sites under any circumstances;
- Staff should not post comments on social networking sites positive or negative about other staff members, pupils or parents.
- Staff should avoid posting anything about school-related matters on personal social media;
- Staff must adhere to when personal mobile phones are allowed to be used - See the Mobile Devices and E- Safety Policy for full expectations.

**Parental Use of Social Networking Sites**

- Parents should **NOT** post photos, videos or comments that include other children at the school;
- Parents should **NOT** use social media on their own devices while on school premises;
- Parents should **NOT** access social media while helping at school or on school visits;
- Parents should raise queries, concerns and complaints directly with the school rather than posting them on social media – whether on their own pages, in closed groups (e.g. groups set up for school parents to communicate with each other) or on the school's pages;
- Parents should **NOT** post anything malicious about the school or any member of the school community.

**Pupil Use of Social Networking Sites**

- Pupils should **NOT** join any social networking sites if they are below the permitted age (13 for most sites including Facebook and Instagram);
- Pupils should tell their parents if they are using the sites, and when they are online;
- Pupils should be aware how to report abuse and inappropriate content;
- Pupils should **NOT** access social media on school devices, or on their own devices while they're at school;
- Pupils should **NOT** make inappropriate comments (including in private messages) about the school, teachers, or other pupils.

This policy is to be used in conjunction with the:

- 'Mobile Devices Policy'
- 'AI Policy' (when approved)

which clearly outlines further expectations around the use of mobile devices and AI technology. All staff will be expected to read and agree both policies.