Great Oaks School e-Safety Policy

Rationale

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

School Internet Use

- All Internet activity during school time should be appropriate to staff's professional activity or the pupil's education;
- All Internet activity by pupils should be supervised by staff;
- All Internet activity is filtered by Exa Networks and Surfprotect;
- 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 Internet 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 Internet 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 school's responsibility;
- The Internet must not be used to engage in any activity for personal gain or personal business transactions;
- The Internet 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 Internet 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;
- Schools are responsible for all e-mail sent and for contacts made that may result in e-mail being received;
- Posting anonymous messages and creating or forwarding chain letters is forbidden;
- 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;
- Messages that contain abusive or objectionable language, that libel others, or that infringe the privacy rights of others are forbidden;
- 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;
- 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;
- 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 **NOT** accept contact from pupils via social networking sites under any circumstances;
- 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.

Use of Mobile Phones

- Students **NOT** are permitted to bring mobile phones into school;
- If a student needs to bring a mobile phone to school it must be handed into the school office at the beginning of the day and collected at the end of the day;
- Staff should have mobile phones switched off in lessons and when on duty, unless they have prior agreement from a member of LMT;
- Staff are advised **NOT** to use their own mobile phones to make work based calls including calls to parents. If in an emergency they are required to do this they should use a number baring facility;
- Staff are **NOT** permitted to take photographs or make recordings in school on their mobile phones;
- Staff in possession of work mobile phones should ensure that they are used primarily for work email, phone calls and access to the calendar. They can, in emergency, be used to make personal or domestic calls but any personal usage must be paid for.

Staff Use of School Owned Laptops and iPads

Staff in possession of school owned laptops and iPads should ensure that they are used primarily for school work. However, staff may use school provided laptops and iPads for personal purposes provided that this never;

- Takes place at the expense of contractual hours;
- Is not used by people other than the staff member;
- Interferes with Great Oaks School work;
- Relates to a personal business interest;
- Otherwise contravenes Great Oaks School's e-Safety Policy.

Acceptable Behaviour when Accessing the Internet or e-Mail from Home Using a School Owned Laptop or iPad

The Internet and email facilities must not be used for;

- The creation, use, transmission or encouragement of material which;
    - is illegal, obscene, libellous or otherwise defamatory
    - is offensive, threatening or annoying to anyone
    - infringes another person's copyright anywhere in the world
    - transmits unsolicited commercial or advertising material
- Obtaining unauthorised access to the school's or the MAT's or another organisation's IT facilities;
- Violating other people's privacy;
- Illegal activities including breaching the Data Protection, Computer Misuse, Obscene Publications Act and Design Copyright and Patents Acts;
- Unauthorised downloading of copyrighted or confidential information;
- Expressing personal views which could be misinterpreted as those of the school.

Date and Signature: _____

Date of Policy: **February 2019**

Date to be reviewed: **February 2021**

Appendix 1 – Form for staff / volunteers to sign

All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with the Head teacher

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will not give out my own personal information such as mobile phone number, personal e-mail address or social network site details to pupils
- I will ensure that personal data is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body. Personal or sensitive data taken off site must be encrypted.
- I will not install any hardware or software on to the school network without permission of the ICT coordinator or a school technician
- I will not browse, download, upload, share or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head teacher. Images should not be taken or stored on staff's own mobile phones, personal iPads or computers
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to my Line Manager or Head teacher.
- I will support the school approach to online safety and not deliberately upload or add any images, video, sounds or text that could upset or offend any member of the school community
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety and Data Security policies and help pupils to be safe and responsible in their use of ICT and related technologies.

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …… Date ……

Print Name……