FALCONHURST SCHOOL

E-SAFETY POLICY

Annual Review to TLS: June 2018
Scheduled Review Date: June 2019

Rationale

This policy applies to the following aspects of ICT

- Websites
- e-mail, Instant Messaging and chat rooms
- Social Media, including Facebook and Twitter
- Mobile phones, Smart phones, tablets and other mobile devices with web functionality
- Gaming, especially online
- Blogging and Vlogging
- Sexting
- Podcasting, Video Broadcasting & Music Downloading.

Whilst exciting and beneficial both in and out of the context of education, ICT is continually being developed, so cannot necessarily be constantly policed. All users need to be aware of the range of risks associated with the use of these technologies. We understand the responsibility to educate our pupils on e-safety issues in order to enable them to remain both safe and legal within and beyond the classroom.

Everybody in the school has a shared responsibility to secure any sensitive information used in their day to day professional duties.

Roles and Responsibilities

As e-safety is an important aspect of strategic leadership within the school, the Head and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

This policy, supported by the school's Staff Code of Conduct for ICT/Acceptable Use Policy for Falconhurst Staff written by the ICT Lead, is to protect the interests and safety of the whole school community. It is linked in principles and practice to the following school policies: Social Networking, Data Protection (GDPR), Safeguarding, Health and Safety, Behaviour (including anti-bullying) and PSHE.E-safety in the Curriculum

IT and online resources are increasingly used across the curriculum. We believe it is essential for e-safety guidance to be given to the pupils on a regular and meaningful basis therefore, e-safety is embedded within our curriculum and pedagogy. All staff should ensure they take every opportunity to promote e-safety across a range of curriculum areas.

Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the PSHE curriculum.

Pupils are taught about copyright ©, respecting other people's information and protecting their own personal information, safe use of images and other important areas through discussion, modelling and appropriate activities.

Pupils are aware of the impact of Cyber bullying and know how to seek help if they are affected by any form of online bullying. Pupils are also aware of where to seek advice or help if they experience problems when using the internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as Cyber Mentors, Childline or CEOP report abuse button.

Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the ICT curriculum.

Pupils are continuously reminded and advised to be aware of PEGI ratings for games and apps as a tool for understanding their suitability. The school will actively remind parents to be vigilant around/avoid PEGI 12+ games and apps in order to collectively safeguard children. Whilst the school accepts that many children socially network, E-safety lessons remind children specifically that platforms such as Facebook, Whatsapp and SnapChat have PEGI ratings older than their Primary School ages.

Pupils with Additional Needs

The school endeavours to create a consistent dialogue with parents for all pupils and this in turn should aid establishment and future development of the school's e- safety rules. However, staff will be aware of some pupils and families who may require additional support or teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil has been identified with social understanding needs, careful consideration is given to group interactions when raising awareness of e-safety. Internet activities will be carefully planned and managed to ensure all children receive resources that are meaningful and age appropriate.

Managing Internet Access

- Passwords must never be shared. Any communications are the responsibility of the owner of the account used.

- School ICT systems security will be reviewed regularly.

- Virus protection will be updated regularly.

- Security strategies are in place. The broadband is constantly filtered as part of our broadband package, in line with DfE requirements. Any filtering issue detected by the filtering software will be logged with the e-Safety or Safeguarding lead for follow-up.

e-mail

The use of e-mail within school is an essential means of communication. In the context of school, e-mail should not be considered private.

The school gives all staff their own e-mail account to use for all school business as a work based tool and is the only account to be used for school business. This is to protect staff, minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed.

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The school email account office@falconhurstschool.co.uk should be the account that is used for all school business and as an initial contact for any whole school or wider community business.

Under no circumstances should staff contact pupils, parents or conduct any school business using personal e-mail addresses.

All e-mails should be written in the same way as a letter written on school headed paper.

We recognise that pupils need to understand how to style an e-mail in relation to their age and good network etiquette. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

e-mails created or received as part of a professional role will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. All e-mail accounts must therefore be actively managed as follows:

- Delete all e-mails of short-term value
- Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- The forwarding of chain letters is not permitted in school.

All pupil e-mail users are expected to adhere to the generally accepted rules of ‘netiquette’ particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in e-mail communications. Staff should remain vigilant and report any concerns immediately regarding pupils’ safety and take every opportunity to remind pupils that agreeing to meet people or giving personal information through e- mail or the internet can be a risk.

IT technicians/contractors are responsible for maintaining virus protection.

e-mails must not be used by any member of the school community to send or receive indecent or offensive images, videos or any written material of this kind. In addition, emails should not be used by any member of the school community to cause intentional harm, upset, directly or indirectly to others.

Pupils must be taught to act immediately and tell a teacher/ trusted adult if they receive an offensive e-mail whether directed at themselves or others and before it is deleted.

Staff must inform the Headteacher if they receive an offensive e-mail whether it is directed at themselves or others and before it is deleted.

Whenever, school e-mail is accessed, (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

All new staff receives information on the Staff Code of Conduct and Acceptable Use Policy for Falconhurst Staff as part of their induction and will sign that they have read, understand and accept the policy.

All staff are made aware of their individual responsibilities relating to the safeguarding of children within the context of e- safety and know what to do in the event of misuse of technology by any member of the school community through induction and CPD.

Staff will preview any recommended sites before use in the classroom and use filtered safe search engines specifically for use by children. ‘Squiggle’ or other Google filtered engines are available.

Raw image searches are discouraged when working with pupils.

If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

All users must observe software copyright at all times. It is illegal to copy or distribute school software or illegal software from other sources.

All users must observe copyright of materials from electronic resources. On-line gambling or gaming is not allowed.

All staff must comply with the Online Presence for Staff Policy regarding the posting of any information or images relating to the school.

Governors and volunteers will also be made aware of this policy with a view to maintaining the reputation of the school.

The school does not allow any access to social networking sites other than the school’s own Facebook page where general information is available for the whole school community and the Twitter feed for live school sports fixtures and updates.

We believe it is essential for parents/carers to be fully involved with promoting e-safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss e-safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

Images and Film

Photographs and film of pupils engaged in school activities can only be stored on school systems and not published on social media without explicit permission of parents/carers. Only first names will be used and no information leading to the identification of a pupil will be provided.

Pupils are not permitted to use personal digital equipment, including mobile phones and cameras in school. Staff must have permission from the Headteacher before any image can be uploaded for publication.

Publishing Pupils’ Images and Work

On a child’s entry to the school, all parents/carers will be asked to give permission to use their child's work/photos for school promotion only.

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

Parents or carers may withdraw permission, in writing, at any time.

Sharing Platforms

With the increased use of the internet, and sharing platforms in particular, the Falconhurst Community need to be aware of the implications of sharing information on these platforms.

- The use of the school logo on any personal web pages is not permitted.
- Please be aware that using material from any copyrighted source without permission is likely to breach copyright.
- The school reserves the right to require removal of any material published by any member of the the Falconhurst Community, or wider which may adversely affect the school's reputation or create risk of legal proceedings against the school.
- Do not include or use any school, data, information, contact details or photographs of employees, pupils, parents or partner organisations without the explicit written permission of the school and the explicit written permission of the data subject (e.g. person shown in any photograph).
- Do not include comments or photographs which could bring into question the schools credibility.
- It is against the school's policy for staff members to accept as 'friends' on social networking sites any child or vulnerable adult, or the family members of any child or vulnerable adult you have met in the course of your employment.
- If you receive press or media contact regarding the content of your personal site and feel there may be implications for you or which in any way relates to the school, you should consult the Headteacher.

Parental Support

The school disseminates information to parents relating to e-safety where appropriate
in the form of:

- Information and celebration evenings
- Practical training sessions
- Newsletter items

Security

The school gives relevant staff access to its Management Information System, with a unique username and password. It is the responsibility of everyone to keep passwords secure; passwords are not to be shared with others and should be changed regularly.

Staff are made aware of their responsibility when accessing school data and have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use. Staff must keep all school related data secure including all personal, sensitive, confidential or classified data or information contained in documents copied, scanned or printed.

Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

ICT equipment issued to staff is logged and serial numbers are recorded as part of the school's inventory. A record of equipment issued and signed for is kept by SBM. Appendix 1.

On termination of employment, resignation or transfer, staff must return all ICT equipment to the school and a signed record kept. Staff must also provide details of all their system logons so that they can be disabled.

Breaches

A breach or suspected breach of policy by a school employee, contractor or pupil may result in the temporary or permanent withdrawal of school ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Policy or Behaviour Policy which could also lead to criminal or civil proceedings.

Incident Reporting

The school's Whistleblowing Policy and Safeguarding Policy can support any member of staff or pupil to report any incident of concern.

E-Safety is the responsibility of all members of the Falconhurst community. Any concerns should be reported to the E-safety or Safeguarding leader.

Protecting Personal Data

Personal data will be recorded, processed, transferred and made available according to the Data Protection Act 2018.