Federation of Trosnant Schools

Head of School: Infant
Tracey Marsh

Executive Headteacher - Ian Waine

Head of School: Junior
Clive Mulligan

Stockheath Lane, Havant, PO9 3BD Tel: 023 92475606 Fax: 023 92499423
Email: adminoffice@trosnant.hants.sch.uk Website: www.trosnantschools.co.uk

Acceptable Use of ICT Policy

Aims and Purposes

To ensure that members of staff are fully aware of their professional responsibilities when using ICT and when working with pupils and parents, they are asked to sign for this code of conduct. Members of staff should consult the school's policy for 'Online Safety', 'IT and Computing' and 'Data Production' policies for further information and clarification.

Systems and Permissions

- I appreciate that ICT includes a wide range of systems, including laptops, tablets, mobile phones, PDAs, digital cameras, email, social networking and that ICT use may also include personal ICT devices when used for school business.
- I know that personal equipment may not be brought onto site and used to replace school items. If something is broken, the IT co-ordinator will endeavour to resolve the issue in good time. Electronic devices may only be brought in with specific permission from the IT co-ordinator and caretaker, and must be PAT tested before use.
- I understand that it is a criminal offence to use a school ICT system for a purpose not permitted by its owner. I will ensure that, when taken home for work use, my laptop and other equipment cannot be accessed by others.
- I understand that access to certain software packages and systems (e.g HCC intranet; SAP (HR, finance and procurement system), SIMS, RAISE Online, FFT, school texting services) will be restricted to nominated staff and unless permission and access has been provided, staff must not access these systems.
- I will respect system security and I will not disclose any password or security information to anyone other than an authorised system manager. I will not use anyone's account except my own. I will not distribute or share personal details of others – in line with the school's Data Protection policy. When using a shared computer, I will ensure I sign out of websites/programs to ensure data is not misused or accessed without permission.
- I understand that I must not use the school ICT system to access inappropriate content at any time. This includes obscene and indecent images, blocked websites (of an adult/mature content, e.g. gambling, betting, gaming, alcohol, tobacco, illegal drugs, auction sites, radicalisation and terrorism, promotion of gang culture or violence).
- I understand that school information systems and hardware (including laptops, iPads issued to staff, cameras and equipment) may not be used for personal purposes without specific permission from the head teacher. I understand that it is my responsibility to look after, keep safe and respect the equipment I have been personally issued, and that I may need to contribute financially to a replacement if this is not deemed to be the case. In addition, we all have collective responsibility for shared items such as laptop trolleys and their contents. Year groups or individual children may receive a ban for inappropriate use or for damaging any shared equipment intentionally. Where appropriate, a child's parents may be contacted and a financial contribution to a replacement device requested.
- I understand that my use of school information systems, Internet and email may be monitored and recorded to ensure policy compliance. The school may exercise its right to monitor the use of the school's information systems and Internet access, to intercept e-mail and to delete inappropriate materials where it believes unauthorised use of the school's information system may be taking place, or the system may be being used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound. This includes connecting to the school wifi system for personal use on mobile phones. In cases where allegations of improper conduct have been made, police involvement may be necessary.
- I will not install any software or hardware from any source without permission.

- I will ensure that sensitive personal data is stored securely and is used appropriately, whether in school or accessed remotely. It must NOT be kept on removable storage devices, taken off premises or kept in cloud storage, e.g. Dropbox, GoogleDrive and iCloud.

- I will respect copyright and intellectual property rights.

- I understand use for personal financial gain, gambling, political activity, advertising, commercial ventures, personal campaigns or illegal purposes is not permitted.

Teaching and Working with Pupils

- I will ensure that I use the school email account I have been provided with solely for the purpose of carrying out my job effectively. I will not use it to communicate with parents or pupils, unless discussed and approved by a member of SLT. My personal e-mail accounts must never be used to conduct school business. The only exception to this is LinkedIn (or other professional networks), where it is acceptable to use an e-mail account that covers both professional and personal use. The office staff reserves the right to access employee's school e-mail accounts if it is anticipated that important communications may be missed due to absence.

- I will not use my mobile phone or hands-free device whilst driving on school business. I understand that I may use my personal mobile phone in exceptional circumstances, such as to contact the school whilst on an off-site visit. I will not use my mobile phone or tablet to take photos of children.

- Any photos of children taken using the school's digital cameras or other equipment must be kept secure and safe. The school has a networked server which can be used to store the images.

- I will ensure I check the content of any video, photo or audio clips I intend to use with children in advance. I must deem it appropriate before use in the classroom. I will disable the auto-play function when watching educational YouTube videos in school.

- I will report any incidents of concern regarding children's safety to the schools Online Safety Coordinator, the designated Child Protection Liaison Officer or Head teacher, using the Reporting Log (found in the IT area or digitally in the IT and Computing folder on Teachers Pool).

- I will promote online safety with students in my care and will help them to develop a responsible attitude to system use, communications and publishing. See Online Safety policy for more details.

- I understand the recent development in the use of online platforms to promote radicalism and extremism to wider audiences, and that I must report any concerns of this nature using the Reporting Log (give to Claire Louth), or if urgent/extreme in nature, Child Protection forms (give to a CPLO).

  Below is an extract from the Prevent Strategy;

  "With varying approaches, the online environment is used to engage and radicalise young people. The use of often slick and professionally-produced propaganda materials, combined with prolific use of Social Media platforms mean that extremist organisations are able to target young people on a scale previously unseen and can exaggerate their scale or influence at relatively low cost. The messages can follow the style of product marketing campaigns including brand recognition and emotional engagement, seeking to exploit vulnerabilities, disillusionment or confused perceptions. Videos and photographs typically feature heavily, and combined with the perceived realtime nature of Social Media, serve to engender a direct link to events.

  Grooming: Often similar to those methods used in online grooming in respect of Child Sexual Exploitation, to develop further engagement, group individuals may encourage the young person to move from the initial 'broadcast' medium (e.g. public forum, one-2-many, social network) to a 'direct' medium (e.g. one-2-one, direct messaging, secure platform). Furthermore, the young person may perceive themselves to be willingly engaged rather than recognising the underlying manipulation or coercion involved. The psychological aspects that surround an individual's susceptibility to be drawn into supporting terrorism are varied, including those factors outlined opposite. The individual's social environment may amplify such vulnerabilities by legitimising and normalising such behaviour. Extremist organisations often employ technology, particularly Social Media, as an ideal medium to engage with a broad audience. The use of technology is often highly articulate, significantly engaging and professionally produced, allowing groups to maximise engagement and seek to legitimise their extremist ideology. As young people are significantly invested in Social Media (though have not necessarily developed the broader life experience and critical thinking skills), they present a particular concern especially where they have particular vulnerabilities which extremist organisations seek to exploit." **Prevent For Schools (P4S: Online Radicalisation), Lancashire Safeguarding Board 2016.**

Personal Use of ICT

- I will make appropriate use of the security settings available on social networking sites and ensure these are updated as the sites make changes themselves. With increasing concerns over identity theft and fraud, I will consider how much personal data is held about me on profiles.

- Only administrative staff and management may use social networking sites as a means of communicating with the school community.

- I will contact a member of the management team if I have any concerns over the safety or security of pupils, staff, parents, equipment or information.

- I understand that the school has an iTunes account which can be used, in consultation with the head teacher and IT co-ordinator, to purchase songs, apps and films. I will not log into my personal iTunes account to download such items, even if this is for an educational purpose. Apps may not be downloaded onto iPads without permission.

Social Media

It is recognised that social networking has the potential to play an important part in many aspects of school life, but staff members must be conscious at all times of the need to keep their personal and professional lives separate. Trosnant Federation respects your right to a private life but has a duty to provide a safe working environment for all stakeholders.

This policy applies to personal webspace, such as social networking sites, blogs, microblogs including Twitter, chat rooms and podcasts and content sharing sites such a Flickr and YouTube.

- I understand the need to exercise extreme care in my personal use of social networking sites. I know that inappropriate communications that come to the attention of school can lead to disciplinary action, including dismissal.

- I will ensure I do not have any pupils or ex-pupils under the age of 18 as friends on social networking sites, including former pupils, and those who have moved to other schools. I will not have any unauthorised contact (electronic) with pupils, current or past, outside of school hours.

- I will not reference pupils, students or parents without their approval.

- I will exercise caution when having contact with, or accepting friend requests from parents.

- I will ensure my comments and posts will not compromise the school's reputation, credibility, information, computer systems or networks. This includes openly identifying themselves as school personnel and making disparaging remarks about the school, its' policies, other staff members and other people associated with the school. I will not express personal views online that the school would not want to be associated with.

- I know that my comments, posts and online activity should not breach any of the policies I have read and signed.

- I will ensure my comments and posts must not be of an illegal, sexual, discriminatory, offensive, hateful, threatening or abusive nature.

- The tone of my comments and posts must not damage relationships with work colleagues in the school, partner organisations, pupils or parents.

- I understand that any harassment of other staff via social media will be investigated by the Senior Leadership Team and may lead to disciplinary action. This includes when the person being targeted is unaware of the comments and posts being made. It is everyone's responsibility to report any such behaviour to either the Computing co-ordinator (Claire Louth) or Senior Leadership Team. It is advised that anyone wishing to report or discuss alleged incidents keep screen-shots, e-mails, text messages or phone logs as evidence. Do not delete any such material. If the concern is in regard to the conduct of the head teacher, this must be disclosed to the chair of governors.

- I understand that the new school blogs will be password protected, and that teaching staff have responsibility for overseeing their class page and approving suitable posts before publishing. Passwords will only be shared with parents and any suspicious activity will be reported.

I have read, understand and accept the staff code of conduct regarding the Acceptable Use of ICT.

Written by Claire Louth (August 2017) in conjunction with the previous policy, guidance provided by Hampshire County Council, including the updated Social Media Policy and Acceptable Use of ICT policies from Education Personnel Services, the Prevent for Schools Strategy, 360 online self-review tool, SWGfL and Lancashire Safeguarding Children Board.

Reviewed: October 2017
Next review date: October 2018 or as required