11-10-17

Streethouse School

Social Media and ICT Acceptable Use Policy for staff, parents and pupils

Social media sites play an important role in the lives of many people, including children. We recognise that social networking can bring many benefits, but there are also potential risks. The aim of this document is to give clarity to the way in which social media sites are to be used by the Streethouse School community: pupils, staff, parents, carers, governors and other volunteers. All members of the school community should bear in mind that information they share through social media and networks, even if it is on private spaces, is still subject to copyright, data protection and Freedom of Information legislation, the Safeguarding Vulnerable Groups Act 2006, and UK libel and defamation laws.

P Wilkins 9-10-17

Staff Guidelines

Computers, laptops and other networked resources, including Internet access, are available to staff in the school. These resources are intended for educational purposes, and may only be used for legal activities consistent with the rules and policies of the school.

It is expected that staff will use computers as appropriate within the curriculum and that they will provide guidance and instruction to pupils in the use of the online curriculum.

The computers are provided and maintained for the benefit of all staff, who are encouraged to use the online resources available to them.

Access is a privilege, not a right and inappropriate use will result in that privilege being withdrawn.

Computers and Laptops at home or school

- Do not install, attempt to install, or store programs of any type (including screen savers and custom mice) on the computers without permission from the network administrator.
- Do not damage, disable, or otherwise harm the operation of computers, or intentionally waste resources.
- Do not use the computers for commercial purposes, e.g. buying or selling goods.
- Do not open files brought in on removable media (such as CDs, flash drives etc.) until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not connect any mobile equipment to the network until they have been checked with antivirus software, and been found to be clean of viruses.
- Do not eat or drink near computer equipment.

Security & Privacy

- Networked storage areas and other external storage hardware (disks etc) are the responsibility of the school.
- Files and communications may be reviewed to ensure that users are using the system responsibly.
- Do not disclose your password to others, or use passwords intended for the use of others.
- Never tell anyone you meet on the Internet personal information, your home address, your telephone number or your school's name, or send them your picture.
- Do not use the computers in a way that harasses harms, offends or insults others. Respect, and do not attempt to bypass, security in place on the computers, or attempt to alter the settings.
- Do not intentionally allow unauthorised access to data and resources on the school network system or other systems.
- Do not intentionally use the computers to cause corruption or destruction of other users' data, or violate the privacy of other users.

Internet

- Do not access the Internet unless for school related activities.
- Do not use the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials, which are unlawful, obscene or abusive.

- Respect the work and ownership rights of people outside the school, as well as other students or staff. This includes abiding by copyright laws.
- Do not engage in 'chat' activities of a personal nature over the Internet including social networking sites, blogs and forums during school time.
- You should not post any e-comments that purport to represent the school unless authorized by the Leadership Team.

Email

- Your Outlook e-mail account will be your principal point of contact for all electronic communication.
- Refrain from using use strong language, swearing or aggressive behaviour.
- Never open attachments to emails unless they come from someone you already know and trust. (They could contain viruses or other programs that would destroy all the information and software on your computer).
- The sending or receiving of email containing material likely to be unsuitable for children or schools is strictly forbidden. This applies to any material of a violent, dangerous, racist, or inappropriate content. (All such messages must be reported immediately to the Headteacher).

Specifically for Laptops for Teachers

- Do not install, attempt to install, device drivers and software on the laptops without permission from the network administrator.
- Access to the school shared network and its resources will only be via laptops that are issued by school.
- No settings must be changed on your laptop unless authorized by the Headteacher; this includes Internet settings, browsers and system preferences.
- You are continuously responsible for the laptop issued. Any damage must be reported to the Headteacher immediately.
- You are responsible for the repair and maintenance costs of laptops (hardware and software) necessary due to negligence or misuse.
- You must not allow any external agency or support service to tamper with school laptops hardware or software.
- Appropriate and safe care and storage of school laptops is expected at home.
- Do not access any other non-internet network from your laptop.
- Laptops must be connected to the network at least once per week to allow updates to occur.

Services

- Streethouse School will endeavour to alert staff of any network related issues that may affect the use of IT within the school network.
- There are no warranties of any kind, whether expressed or implied, for the network service offered by the school.
- The school will not be responsible for any loss of data as a result of service interruptions from external systems and providers including the internet service providers, server malfunctions or delay and non-delivery of devices and or software.
- Use of any information obtained via the network is at your own risk.

Use of social media sites by employees in a personal capacity

It is possible that a high proportion of staff will have their own social networking accounts. It is important that they protect their professional reputation, and that of the school, by ensuring that they use their personal sites in an appropriate manner.

Staff will be advised as follows:

- That they familiarise themselves with social network sites' privacy settings in order to ensure that information is not automatically shared with a wider audience than intended It is recommended that, as a minimum, all privacy settings are set to 'friends only', irrespective of use/purpose
- That they do not conduct or portray themselves, or allow friends to portray them, in a manner which may bring the school into disrepute; lead to valid parental complaints; be deemed as derogatory towards the school and/or its employees; be deemed as derogatory

towards pupils, parents/carers or governors bring into question their appropriateness to work with children contravene current National Teacher Standards
- That they do not form online friendships or enter into communication with parents/carers as this could lead to professional relationships being compromised
- That they do not form online friendships or enter into online communication with pupils as this could lead to professional relationships being compromised, and/or safeguarding allegations being raised
- That they should not post pictures of (without the Headteacher's consent) or negative comments about school events
- That if their use of social media/networking sites contravenes this policy, they may be subject to disciplinary action

Inappropriate use by employees should be referred to the Headteacher in the first instance.

Creation of social media accounts by school staff for use in education
All social media services must be approved by the Headteacher in advance of any educational work being undertaken.

Comments posted by parents/carers on social media sites
- Parents/carers will be made aware of their responsibilities regarding their use of social media via this policy (in particular when their child joins the school), the school website, letter and school newsletters.
- Parents/carers are asked not to post images (photos and videos) of pupils other than their own children on social media sites unless they have the permission of parents of other children pictured
- Parents/carers are asked to raise queries, concerns or complaints directly with the school rather than posting them on social media
- Parents/carers should not post malicious or fictitious comments on social media sites about any member of the school community

Dealing with incidents of online (cyber) bullying
There are four UK statutes that cover the use of Internet technology in relation to bullying. All cases of online bullying will be dealt with in accordance with the school's Anti-Bullying policy. The school can take action with reference to any incident that takes place outside school hours if it:
- Could have repercussions for the orderly running of the school
- Poses a threat to a member of the school community
- Could adversely affect the reputation of the school, or its employees/governors

Where appropriate, legal action will be taken by the school's governors.

Signed : _____ Date : _____

Chairperson of the Governing Body

Signed : _____ Date : _____

Headteacher