

# Staff Acceptable Use for E-Safety Policy & Social Networking Standards

## September 2017

Tapton School recognises that the use of ICT, internet, the Learning Platform and a wide range of electronic communication can greatly enhance the quality of learning across our school community. It is vital that every member of staff fully understands and adheres to the required policy that ensures safe, appropriate and responsible use of such technologies. Please take time to read this agreement carefully and make sure you fully understand each point before signing the agreement.

- I will keep my login, email address and password confidential. I will take care to ensure that others cannot use my accounts to access confidential information about students or staff by always logging off when I have finished work or locking my computer when it is left unattended.
- I will never use anyone else's login, email address or password or access their work without their permission.
- To protect my own privacy I will use a school email address and school telephone numbers (including school mobile phone) as contact details for students and their parents.
- Any form of electronic communication with students or parents will only be via the school's accredited system or Learning Platform.
- I will ensure that all communication, including communication via social networking sites (e.g. Face book) is transparent and open to scrutiny.
- I will ensure that communication between myself and students, by whatever method, should take place with clear and explicit professional boundaries. "Think before you Post!"
- I understand that the use of the network or any school device to knowingly access inappropriate materials such as pornographic, racist or offensive material is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to material which might be considered unacceptable immediately to my line manager and ensure it is recorded and notify my line manager if I suspect someone else of misusing ICT facilities or the internet.
- I understand that I must also inform the designated Child Protection Liaison Officer if misuse may be a child protection issue.
- I will ensure that students under my supervision use ICT facilities and the internet appropriately to support learning. I will challenge and report any misuse.
- I will screen all USB pens, digital media and portable devices for malicious software before I download any files to the network and take care when opening unknown email attachments. I will seek advice from the ICT strategy manager if I am unsure about the safety of any such devices or attachments.
- I will not attach any devices to the network which may contain files which breach copyright, data protection or other laws.
- I agree to use the school's ICT facilities and internet only for work related use during my working hours (excluding designated breaks).
- I will take all reasonable steps to ensure the safety and security of school ICT equipment which I take off site and will remove anything of a personal nature before it is returned to school.
- I will only use my mobile phone during non-teaching time. It will be turned off or kept on silent mode during lessons except in an emergency situation with the agreement of a member of the Senior Leadership Team.
- I will only use my mobile phone or other electronic equipment to photograph or video students as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage never leaves school premises.
- I understand that the school reserves the right to check files and monitor the internet sites used by staff.
- I understand that the misuse of ICT facilities and the internet could result in disciplinary action being taken against me.

### **Staff social networking standards**

Below sets out the standards expected of all staff representatives when using social media.

## DO

- Act responsibly at all times. Even if you do not identify your profession or place of work, please be aware that your conduct online could jeopardise any professional registration and/or your employment
- Protect your own privacy. Think about what kind of information you want to share online and who you want to share this with. Adjust your privacy settings accordingly.
- Remember everything is public. Even with the highest level of privacy settings, once something is online it can be copied and redistributed and it is easy to lose control of the information. Work on the assumption that everything you post online will be permanent and will be shared with others.
- Take appropriate action if you are the target of abuse online. If you are the target of bullying or abuse online you can take action in dealing with this, such as blocking individuals from interacting with you and reporting inappropriate activity.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual concerned. Always remove information about a colleague if they ask you to do so.
- Respect the privacy of others. If photographs are taken at an event then check whether those in attendance expect that any photos may appear on a public social networking site before posting. Remember it may not always be an appropriate way to share information whether work related or not.
- Remember the benefits. Used responsibly, social media can be accessed to keep up to date with a number of professions and information.

## DO NOT

- Share confidential information online. In line with the Data Protection Act 1998 employees should not share any child / family identifiable information online or any personal information about colleagues. In addition to this, any confidential information about the school should not be revealed online.
- Build or pursue relationships with children, parents, families. Even if the child / client or parent is no longer within your care, the school does not deem this as appropriate behaviour. If you receive a request from a child / client or parent then many sites allow you to ignore this request without the individual being informed to avoid any offence. If you are concerned about this in any circumstance, please discuss with your Line Manager.
- Use social networking sites to inform professional practice. There are some circumstances/job roles where this may be appropriate, however careful consideration and discussions with management should be applied.
- Discuss work related issues online. This takes into account conversations about parents, children, colleagues or anything else which may identify the school online and bring into potential disrepute. Even if you think these conversations have been anonymised they are very likely to be deemed inappropriate.
- Post pictures of children/young people/their parents. Never post pictures of clients / parents or their children online even if they have asked you to do this. Employees should never take pictures of parents, children unless they are relevant and within the boundaries of the digital images policy. Permission from the subject and parents of children should always be obtained. *If your mobile phone has a camera then this should not be used in the workplace except if permission has been given by a member of the Senior Leadership Team.*

- Raise concerns about your work. Social networking sites should never be used for raising or escalating concerns at work. If you have concerns then these should be raised through either discussing with your line manager or following the relevant policy/procedure for raising concerns at work.
- Engage in activities online which may bring the Organisation into disrepute. Think through what activities you take part in whilst online and what you do or say that may bring the school into disrepute. Any reports of this will be reviewed in line with their appropriateness.
- Be abusive to or bully other colleagues. Social networking sites should not be used as a forum for abusive behaviour towards colleagues.
- Post derogatory, defamatory or offensive comments about colleagues, the child / parents / clients / families, or school. Everything posted on a social networking site should be deemed as open to the public and it is therefore unacceptable to use this as a forum for posting inappropriate comments.

All of the above apply to both open and private sections of any social networking site employees identify themselves with.