Milborne St Andrew First School

Staff Internet and Mobile Phone Code of Conduct Policy

Document Detail	
Policy Reference Number:	
Category:	Staff internet code of conduct Safeguarding
Authorised By:	Local Governing Body
Author:	Richard Scott DASP
Version:	
Status:	Approved January 2017
Next Review Date:	Jan 2018

A Code of Conduct for Staff Internet and Mobile Phone use

DASP
Getting it right
for every child
by working together

Protect your personal identity

Looking after your personal details is obviously important in all aspects of life. For a teacher, or anyone dealing with young people, it is perhaps even more so. This guidance is intended to work in support of a School Policy that ensures responsible use of computers, the internet and mobile technology by staff and students. Rules or guidance in a school policy are for protection, not punishment or control. All staff have Rights to privacy and protection, but they also have responsibilities to use the internet and other technologies responsibly to ensure this. **DCSF** Guidance states:

‘Communication between children and adults, by whatever method, should take place within clear and explicit professional boundaries. This includes the wider use of technology such as mobile phones text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.

Adults should not share any personal information with a child or young person. They should not request, or respond to, any personal information from the child/young person, other than that which might be appropriate as part of their professional role

Adults should ensure that all communications are transparent and open to scrutiny.’

The main areas to consider are:

Online internet use at school and home, including social networking
Mobile phones
Cyberbullying
Pupil data

It might seem that including home use is irrelevant, as that is your own business and nothing to do with school. However, the nature of the internet and the fact that it is, in reality, a public place means that you need to exercise as much care at home as at school. In fact, in many respects more care, as your home system will not have the filtering in place that we are used to in schools.

So what situations can arise that put a member of staff at any kind of risk?

Social Networking

Many members of school staff now use sites such as Facebook. There have been issues of students seeing photos of the Christmas social and a less than professional view of the staff. If in doubt, don’t upload the photos. Some teacher’s Facebook sites have been ‘cloned’ or faked by students, who then use this to either gain access to other members of staff’s personal sites or to pretend to be that member of staff and publish unsuitable comments. Users should make sure they are completely familiar with the privacy settings policy in place.

It is also recommended very, very strongly that members of a school staff do not have students as ‘friends’ on their Facebook site. This can open staff up to all sorts of risks of inappropriate conduct or comments or being falsely accused of such. It is also recommended that you do not have parents as Facebook contacts. This may be difficult when they are, in fact, friends or acquaintances in ‘real life’. However, remember that the friend/parent you know will have other parents as Facebook friends that are not yours. Yet there is a real possibility that they will see comments you made, supposedly in confidence. And some parents may lead you into making comments about the school online, that you regret later. So it is better not to open yourself to such problems.

Social Networking sites tend to encourage a quick, sometimes unthinking expression of thoughts. In general chat, this is not a major problem. However, imagine some of the conversations you might have with someone in the staffroom about a child becoming public. This has been known to happen, when a member of staff, ‘chatting’ on Facebook expressed views that were seen by other parents. As in all things, common sense is the guide; stop and think before you ‘say’ something on a social networking site. You can also make it clear to parents, that a refusal to accept them as Facebook friends is a professional, school policy decision and not intended to offend.

School computers and Internet use

Most staff will now have a school laptop or iPad, which take home. This has become an essential part of a teacher’s work life. With its advantages come a number of responsibilities. Remember that a school device, used at home, is still a school machine and should be used appropriately. This should all be covered by the schools acceptable use policy. A school must decide what private use staff can make of a school computer either at home, or out of lesson time at school. For example, do you allow staff to book holidays on a school machine or use social networking sites? Remember that many online computer games could bring you into contact with young people. Obviously there will be some areas where staff access would certainly not be allowed. The issue of viruses needs to be considered, when accessing non educational websites. Remember also, that if other members of your family have access to a school laptop at home, they need to be aware of responsible use.

You should also be careful about entering personal details about yourself on any website. At best, your details will go to a telephone sales company and you will get that call about insurance or a survey, just as you sit down to dinner. At worst, your personal and financial details may go to criminals and be used in computer fraud. Security of a website is usually indicated either by a small padlock icon at the bottom of the screen, or by the website address beginning https rather than http.

Ensure that your computer is up to date with its virus checker and it is working. You need to be careful of ‘spoof’’ websites or messages that require you to logo on to somewhere. A popular one is the message that tells you your computer has viruses and you need to do a scan. These are intended to get you to supposedly buy a virus checker, but in reality, are to gain your financial details or put even more viruses on your computer. Such scams have also recently started coming via phone calls as well.

And remember, at school, do not leave your computer logged in and unattended. It could be used to send or receive unsuitable material by someone else, but you will be blamed.

Mobile Phones

It should now be a standard part of school policy that staff do not use their own phone to communicate with students, parents or to take videos or photos of students. It is realised that, with the photo issue in particular, this can be contentious as there can be a situation on a school trip where it is the only thing available to get an important photo. Schools can have wording in the policy that describes what staff do in that situation. This would normally be to take the photo, but to download it as soon as they are back in schools, then immediately delete it from the phone. Ideally though, a school should have a mobile phone that staff can take with them and return to school at the end of the trip. Again, this policy is to protect staff and to ensure that parents see the school policy is transparent. Remember that, if you use your mobile, even just to text a message to a parent, they then have your number (and possibly their child also then has it and can spread it around).

As a side note, it is good practice for staff to respect school rules about mobile use. It is advisable not to use them publically where students are forbidden from using them, as this can cause resentment. Also ensure you have 'Bluetooth' switched off (check phone settings on your mobile), as this allows other users to 'see' your phone, including your address book. It is a good idea to record your phones International Mobile Equipment Identity, in case it is stolen or missing. You can do this by typing:

***#06#**

If your phone is e-mail enabled, you should consider making sure you use pin number protection to restrict access. If your phone is lost or stolen, others have access to information in your e-mails, or to send e-mails or texts in your name.

Cyberbullying

Cyberbullying is well known as a problem amongst children, but it can also be a big problem for staff. We have already looked at how websites can be used to gain access to teachers or make them appear to be making inappropriate comments. However, internet sites and mobile phones can also be used to persecute members of staff. Whilst this will be upsetting and frustrating, staff should deal with it in an appropriate way that is hopefully supported by school policy. Staff should be able to expect that the school will take their claim seriously and respond to any incident.

The guidance to anyone in this situation is:

Don't retaliate with your own messages.
Inform your line manager/Head teacher
Keep all messages, e-mails, screens etc. and make sure they are dated.

The school would then look at this and decide if it can be dealt with internally. It should know that any physical threats are illegal and must be reported to the police. If in doubt, a school could contact the South West Grid for Learning for advice.

Pupil Data

These days a large amount of data is collected on student progress and achievement and so teachers end up carrying this around with them for study and evaluation. We must remember that this data is personal to that student and legally, is subject to the Data Protection Act. For that reason, it is very strongly recommended that password protection is used to access staff computers and that this login is not given out to anyone else. It is also possible to encrypt particular files so they can only be accessed by password. If memory sticks are in use to transport pupil data and work, then these should be encrypted as well. A school (and the teacher responsible) will be in trouble if a memory stick is lost that contains such data. It is hard to say which would be the worse situation – a student finding the memory stick or a local reporter.

Consider also that it is not only data on pupils to take care with. If you keep information about yourself on laptops and memory sticks you should encrypt this. Ideally, not keeping data on computers which go outside school or on memory sticks will reduce the risk of it falling into the 'wrong' hands.

Summing up

Feb 2017 AA

Ensure that the school Acceptable Use Policy (AUP) covers these issues and gives clear guidelines to staff and a methodology for responses to problems. Such a policy should cover staff and student use of new technology, with a consistent approach to both. The document should also cover the schools policy towards using photos and videos on websites and in school.

Ensure that parents are kept informed of these policies and the possible responses. Not only so they know why you might seem 'unfriendly' on line, but also so they know the school takes the safety of children and staff very seriously.

Try Googling your name (using inverted commas e.g. "Fred Bloggs") every now and then. This is not an ego boost, but will see if your name is being used by others.

This document is not intended to terrify you and make you give up all new technology! However, just as we have a duty to ensure students are safe and secure when online, we should also protect ourselves. If you act responsibly and follow school policies, you should avoid problems. Use common sense; don't put yourself in any online situation where you might be at risk.

Sources of information

DASP Website

www.dasp.org.uk/e-safety.htm

DCSF Guidance

Guidance for Safer Working Practice for Adults who Work with
Children and Young People

www.dcsf.gov.uk/everychildmatters/resources-and-practice/IG00311/

South west Grid for Learning

http://www.swgfl.org.uk/Staying-Safe

Richard Scott
E-Learning Manager
DASP

September 2010