Employee Advice on the use of Electronic Communications and Social Media

Contents

1. Introduction

We understand that the use of electronic equipment and social media helps our school to provide a quality service but we also realise that if not used correctly these can be very detrimental to the school and possibly to you. We want you to feel confident when using this equipment so, these guidelines have been put together to help ensure that all of us are aware of our responsibilities and to help us understand good practice when using the schools electronic equipment and social media.

It is important that you take time to read this document and keep it in mind at all times because **failure to follow any aspect of these guidelines (either deliberately or accidentally) could lead to disciplinary action against you in line with the schools disciplinary policy which may result in dismissal.**

2. What is Electronic Communication equipment?

Electronic communications equipment includes things such as your mobile phone, voicemail, the schools fax and photocopying machine, computers, the laptop school have given you, digital camera, palm held devices and it includes email and internet to name but a few things.

3. What is Social Media?

We use the term “social media” to describe any kind of tool that you can use for sharing what you know, including (but not limited to): blogs, photo sharing, video sharing, social networks, mobile phone applications, texting, digital TV services, wikis, gaming and collaboration tools.

Remember - it's the way you use it that makes it social.

4. Personal use of electronic communication

We allow employees to use this equipment for appropriate and moderate personal use. We trust employees to behave sensibly and to use equipment for reasonable and appropriate personal use outside of recorded working time. (For example, using the internet or sending emails at lunchtime or after school hours).

5. Personal use of social media

It's your own personal choice whether or not you choose to participate in any kind of social media activity in your own time – the views and opinions that you express are your own. However, as a school employee you should be aware that any information which you post about school cannot be kept entirely separate from your working life.

There have been occasions where employees have found themselves in a disciplinary process because of something they posted online.

What you say openly online can be accessed around the world within seconds, it might be shared or re-published elsewhere (online or in print) and it will continue to be available for all to see in the future. You must be willing to take personal responsibility for anything that you say online.

As someone working in a school you need to be especially careful and very much aware of the fact that colleagues, parents, management and pupils could access your information including personal photographs.
As well as the potential for young people you work with to contact you, you also need to be aware of accidentally bringing your workplace or your professional role into disrepute through inadvertently posting inappropriate comments about work on your profile, for instance criticising policy or fellow colleagues.

6. Some tips for the safe use of electronic equipment and social media

- Check your online privacy settings so that you understand who can see the information you publish and who can view your personal information.
- Think about what capacity you're speaking in, particularly if you are commenting about school. Make sure you avoid misunderstandings about whether you're speaking as part of your work or not.
- Add a disclaimer to your blog or social media profile to make it clearer that your personal accounts are personal – for example: 'These views are my own and do not necessarily represent the views of the school'
- Respect privacy and confidentiality – make sure you don't publish any information that should be kept private.

Remember; if in doubt don't post it!

- **Mind your language!** All work communications should be written in a professional tone.
- **Your security** - An individual should not access the email of another individual within the school without express permission and a clear understanding of the reason for the proxy access. However, staff should be aware that school email accounts may be accessed by other school staff for monitoring or management purposes. Always keep a copy of email

communications with pupils and parents (whether sent or received) and keep a note of the dates, times and content of telephone conversations.

- Make sure your electronic equipment is password protected so that other people cannot access your information/equipment. Keep your password and login details private!
- Don't open an email attachment unless you have confidence in its origin as this is one of the most likely points of access of a virus into the school's computer systems.
- If you receive an inappropriate an email - offensive, obscene and/or discriminating – you must to report it immediately, and in writing, to the designated person in school (or the head teacher). Where possible, a copy of the email should also be provided and the email and any attachments must be deleted.
- **Stay safe** – don't give out personal details such as your address or phone number. Never use your own personal communications device, such as a mobile phone, or personal email to communicate with pupils or parents because, once your identity is known, you are open to harassment through unwanted phone calls, text messages and emails. A number of cases of parents and pupils bullying teachers in this way have been reported.
- Never use a personal electronic equipment to take images of pupils. Once uploaded, any images should be deleted from the camera's memory. Photographs of children should not be taken home to use on a personal computer.

7. Misuse of electronic equipment

Social media and electronic communications are constantly changing so, it is impossible to give you a definitive list of what not to do. The list below is intended simply as a guideline.

Employees **MUST NOT** use school equipment to:

- Store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred
- Use obscene language or swear words in your communications. Do not communicate messages which are critical about members of the school community including pupils, contain specific or implied comments you would not say in person or contain inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual orientation.
- Gamble using school equipment
- Undertake political lobbying
- Promote or run a commercial business
- Download or distribute games, music or pictures from the internet for personal use. They can bring viruses with them, use up capacity on the servers and potentially breach copyright.
- Use school electronic equipment during work time. This may be treated as fraud.

- Store personal information on your system or network that uses up capacity and slows down the system (for example, personal photos, screensavers or wallpaper)
- Conduct private and intimate relationships via email
- Download or copy software (excluding software updates) onto school equipment or use the email system to transmit any documents or software without checking copyright or licence agreement
- Install software licensed to the school on a personal computer at home unless permission to do so is explicitly covered by the school licence agreement.

This list is not exhaustive.

8. Monitoring and Privacy

The school's email and internet facilities are business systems, owned by the organisation. The school therefore reserves the right to track all use of the internet and of the school's IT systems. Usage will be monitored to ensure that the systems are being employed primarily for business & educational reasons, that there is no harassment or defamation taking place and, that employees are not entering into illegal transactions.

Employees need to be aware that internet sites visited are traceable, and that deleted or trashed messages or attachments can be recovered.

Email, telephone calls and internal and external post (unless clearly identified as private and confidential post) should be used primarily for business and educational reasons, to ensure this, monitoring will be carried out on a regular basis. School managers have proxy access to all the school's communication systems for monitoring and interception of communications in order to deal with matters in an employee's absence for holiday, illness or other reason

Any material stored on the school's network or being circulated via the school's email system has no rights of individual privacy. In accordance with RIPA (Regulation of Investigatory Powers Act 2000) monitoring or surveillance without an employee's knowledge can be carried out on internal email systems, or information stored on a server.

9. Breaches and Sanctions

Failure to follow any aspect of these guidelines (either deliberately or accidentally) could lead to disciplinary action against you in accordance with the school's disciplinary policy which may result in dismissal.