2.13 – IT and Communications Systems Policy

1. About this policy

1.1. Our IT and communications systems are intended to promote effective communication and working practices when working in any Academy of the Trust. This policy outlines the standards you must observe when using these IT and communication systems, when we will monitor their use, and the action we will take if you breach these standards.

1.2. The Trust has overall responsibility for this policy, including keeping it under review.

1.3. Breach of this policy may be dealt with under our Disciplinary Procedure and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.4. This policy does not form part of any employee's contract of employment.

2. Equipment security and passwords

2.1. You are responsible for the security of the equipment allocated to or used by you, and you must not allow it to be used by anyone other than in accordance with this policy. You should use passwords on all IT equipment, particularly items that you take out of Academy. You should keep your passwords confidential and change them regularly.

2.2. You must only log on to our systems using your own username and password. You must not use another person's username and password or allow anyone else to log on using your username and password.

2.3. If you are away from your desk or the computer you are working from then you should log out or lock your computer. You must log out and shut down your computer at the end of each working day.

3. Systems and data security

3.1. You should not delete, destroy or modify existing systems, programs, information or data (except as authorised in the proper performance of your duties).

3.2. You must not download or install software from external sources without authorisation from your Headteacher or the Trust. Downloading unauthorised software may interfere with our systems and may introduce viruses or other malware.

3.3. You must not attach any device or equipment including mobile phones, tablet computers or USB storage devices to our systems without authorisation from your Headteacher or the Trust.

3.4. We monitor all e-mails passing through our system for viruses. You should exercise particular caution when opening unsolicited e-mails from unknown sources. If an e-mail looks suspicious do not reply to it, open any attachments or click any links in it.

3.5. Inform your manager or the Headteacher immediately if you suspect your computer or any Academy computer or IT equipment may have a virus.

4. **E-mail**

4.1. Adopt a professional tone and observe appropriate etiquette when communicating with third parties by e-mail. You should also include our standard e-mail signature and disclaimer.

4.2. Remember that e-mails can be used in legal proceedings and that even deleted e-mails may remain on the system and be capable of being retrieved.

4.3. You must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, pornographic or otherwise inappropriate e-mails.

4.4. You should not:

4.4.1. send or forward private e-mails at work which you would not want a third party to read;

4.4.2. send or forward chain mail, junk mail, cartoons, jokes or gossip;

4.4.3. contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to others who do not have a real need to receive them; or

4.4.4. send messages from another person's e-mail address (unless authorised) or under an assumed name.

4.5. Do not use your own personal e-mail account to send or receive e-mail for the purposes of our multi-academy trust. Only use the e-mail account we have provided for you.

5. **Using the internet**

5.1. Internet access is provided primarily for school purposes only. Occasional personal use may be permitted as set out in paragraph 6.

5.2. You should not access any web page or download any image or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content that is legal in the UK may be in sufficient bad taste to fall within this prohibition. As a general rule, if any person (whether intended to view the page or not) might be offended by the contents of a page, or if the fact that our software has accessed the page or file might be a source of embarrassment if made public, then viewing it will be a breach of this policy. Occasionally legitimate websites are hacked and someone following a legitimate link may be redirected to inappropriate content – in which case employees should immediately advise the Headteacher or appropriate IT colleague in writing as soon as the incident occurs.

5.3. We may block or restrict access to some websites at our discretion.

6. **Personal use of our systems**

6.1. We permit the incidental use of our systems to browse the internet and make personal telephone calls subject to certain conditions. Personal use is a privilege and not a right. It must not be overused or abused. We may withdraw permission for it at any time or restrict access at our discretion.

6.2. Personal use must meet the following conditions:

6.2.1. it must be minimal and take place outside of normal working hours (that is, during your lunch break, and before or after work);

6.2.2. personal e-mails should be labelled "personal" in the subject header;

6.2.3. it must not affect your work or interfere with the of the Trust or the Academy where you work;

6.2.4. it must not commit us to any marginal costs; and

6.2.5. it must comply with our policies including the Equal Opportunities Policy, Anti-harassment and Bullying Policy, Data Protection Policy and Disciplinary Procedure.

7. Monitoring

7.1. Our systems enable us to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in our role as an employer, your use of our computer systems (including any personal use) may be continually monitored by automated software or otherwise.

7.2. We reserve the right to retrieve the contents of e-mail messages or check internet usage (including pages visited and searches made) as reasonably necessary in the interests of the Trust, including for the following purposes (this list is not exhaustive):

7.2.1. to monitor whether the use of the e-mail system or the internet is legitimate and in accordance with this policy;

7.2.2. to find lost messages or to retrieve messages lost due to computer failure;

7.2.3. to assist in the investigation of alleged wrongdoing; or

7.2.4. to comply with any legal obligation.

8. Prohibited use of our systems

8.1. Misuse or excessive personal use of our telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Procedure. Misuse of the internet can in some cases be a criminal offence.

8.2. Creating, viewing, accessing, transmitting or downloading any of the following material during work time, or on Academy business, or using

Academy equipment - will usually amount to gross misconduct (this list is not exhaustive):

8.2.1. pornographic material (that is, writing, pictures, films and video clips of a sexually explicit or arousing nature);

8.2.2. offensive, obscene, or criminal material or material which is liable to cause embarrassment to us;

8.2.3. a false and defamatory statement about any person or organisation;

8.2.4. material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy or our Anti-harassment and Bullying Policy);

8.2.5. confidential information about us or any of our pupils, parents, Academy Councillors, trustees, staff or suppliers (except as authorised in the proper performance of your duties);

8.2.6. unauthorised software;

8.2.7. any other statement which is likely to create any criminal or civil liability (for you or us); or

8.2.8. music or video files or other material in breach of copyright.

2.14 – Social Media Policy

1. **About this policy**

1.1. This policy is in place to minimise the risks to the multi-academy trust through use of social media.

1.2. This policy deals with the use of all forms of social media, including Facebook, LinkedIn, Twitter, Google+, Wikipedia, Whisper, Snapchat, Instagram, Vine, Tumblr and all other social networking sites, internet postings and blogs. It applies to use of social media for business purposes as well as personal use that may affect our organisation in any way.

1.3. The Trust has overall responsibility for this policy, including keeping it under review.

1.4. This policy does not form part of any employee's contract of employment.

2. **Prohibited use**

You must not:-

2.1. access social media sites for personal use via Academy information systems or using Academy equipment (unless you have obtained prior written consent from the Headteacher);

2.2. place inappropriate photographs or post indecent comments or remarks on any social media site;

2.3. make any social media communications that could damage the interests or reputation of the Trust, even indirectly;

2.4. use social media to defame or disparage us, our pupils, parents, staff or any third party;

2.5. post any photograph of any current pupil (unless you have obtained prior written consent from the Headteacher);

2.6. use social media to harass, bully or unlawfully discriminate against pupils, parents, staff or third parties;

2.7. use social media to make false or misleading statements; or to impersonate colleagues or third parties;

2.8. express opinions on our behalf via social media. You may be required to undergo training in order to express such views;

2.9. post comments about sensitive Academy-related topics, such as our performance, or do anything to jeopardise our trade secrets, confidential information and intellectual property;

2.10. disclose any information about the Academy or the Trust which is considered confidential;

2.11. include our logos or other trademarks in any social media posting or in your profile on any social media.

2.12. offer or accept current pupils or ex-pupils as friends on any social media site – personal communication could be considered inappropriate and unprofessional and makes staff very vulnerable to allegations. If you receive any message on any social networking that you believe may be from a pupil or ex-pupil then you must not reply and must report it to the Headteacher immediately.

3. You should ensure that your privacy settings are set to maximum privacy and any social networking is private for your known contacts only.

4. You are advised to act with caution when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites can blur the lines between work and personal life and it may be difficult to maintain professional relationships or it may be just too embarrassing if too much personal information is known in the work place;

5. The contact details of contacts made during the course of your employment are our confidential information. On termination of employment you must provide us with a copy of all such information, delete all such information from your personal social networking accounts and destroy any further copies of such information that you may have.

6. **Guidelines for responsible use of social media**

6.1. You should make it clear in social media postings, or in your personal profile, that you are speaking on your own behalf. Write in the first person and use a personal e-mail address.

6.2. Be respectful to others when making any statement on social media and be aware that you are personally responsible for all communications which will be published on the internet for anyone to see.

6.3. If you disclose your affiliation with us on your profile or in any social media postings, you must state that your views do not represent those of your employer (unless you have been authorised to speak on our behalf as set out above). You should also ensure that your profile and any content you post are consistent with the professional image you present to colleagues and third parties (including parents).

6.4. If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from posting it until you have discussed it with your Headteacher.

6.5. You should immediately report any misuse of social media (by you or any colleague) to your Headteacher.

6.6. If you see social media content that disparages or reflects poorly on us, you should contact your Headteacher immediately.

6.7. Any social media posting must:-

6.7.1. be conscientious and loyal to the aims and objectives of the Trust and the Academy where you work; and

6.7.2. have regard to, maintain and develop the Church of England character of the School; and

6.7.3. not do anything which is in any way detrimental, prejudicial, or contrary to the interests of the Trust or the Academy where you are principally employed to work.

7. Breach of this policy

7.1. The Trust monitors usage of its internet and email services without specific notification or authorisation from users.

7.2. Breach of this policy may result in disciplinary action up to and including dismissal. Any member of staff suspected of committing a breach of this policy will be required to co-operate with our investigation, which may involve handing over relevant passwords and login details.

7.3. You may be required to remove any social media content that we consider to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.