Michaela Community School

IT and Communication Systems Policy

1 ABOUT THIS POLICY

1.1 Michaela Community School's IT and communications systems are intended to promote effective communication and working practices within our organisation. This policy outlines the standards that all staff must observe when using these systems, the circumstances in which the School will monitor use, and the action it will take in respect of breaches of these standards.

1.2 Misuse of IT and communications systems can damage the School and its reputation. Breach of this policy may be dealt with under the School's Disciplinary Policy and, in serious cases, may be treated as gross misconduct leading to summary dismissal.

1.3 This policy does not form part of any employee's contract of employment and it may be amended it at any time.

2 EQUIPMENT SECURITY AND PASSWORDS

2.1 All staff are responsible for the security of the equipment allocated to or used by them, and must not allow it to be used by anyone other than in accordance with this policy.

2.2 Staff are responsible for the security of any computer terminal used by them. Computer terminals should be locked or logged off when left unattended or on leaving the office, to prevent unauthorised users accessing the system. Anyone who is not authorised to access our network should only be allowed to use terminals under supervision.

2.3 Staff should use passwords on all IT equipment, particularly items that they take out of the office. Staff must keep passwords confidential and change them regularly. Staff must not use another person's username and password or make available or allow anyone else to log on using their username and password. On the termination of employment (for any reason) staff must provide details of their passwords to [POSITION] and return any equipment, key fobs or cards. Staff MUST NOT:

2.3.1 Eat or drink close to computer equipment.

2.3.2 Leave equipment unattended in either a public place or a vehicle. (If leaving equipment in a vehicle is unavoidable, it must be stored securely out of sight and the vehicle must be locked.)

2.3.3 Leave portable computers in an unsecured environment either in or out of the School.

3 SYSTEMS AND DATA SECURITY

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

3.2 Staff must not download or install software from external sources. Incoming files and data should always be virus-checked by the IT Technician before they are downloaded. If in doubt, staff should seek advice from the IT Technician.

3.3 Staff must not attach any device or equipment to the School's systems without authorisation from IT Technician. This includes any USB flash drive, MP3 or similar device, PDA or telephone, whether connected via the USB port, infra-red connection port or in any other way.

3.4 The School monitors all e-mails passing through its system for viruses. Staff should exercise particular caution when opening unsolicited e-mails from unknown sources or an e-mail which appears suspicious (for example, if it contains a file whose name ends in .exe. The School reserves the right to delete or block access to e-mails or attachments in the interests of security. It also reserves the right not to transmit any e-mail message.

3.5 Staff should not attempt to gain access to restricted areas of the network, or to any password-protected information, except as authorised in the proper performance of their duties.

4 E-MAIL

4.1 Although e-mail is a vital business tool, staff should always consider if it is the appropriate method for a particular communication. Correspondence with third parties by e-mail should be written as professionally as a letter. Messages should be concise and directed only to relevant individuals.

4.2 Staff must not send abusive, obscene, discriminatory, racist, harassing, derogatory, defamatory, or otherwise inappropriate e-mails. Anyone who feels that they have been harassed or bullied, or are offended by material received from a colleague via e-mail should inform their line manager.

4.3 Staff should assume that e-mail messages may be read by others and not include anything which would offend or embarrass any reader, or themselves, if it found its way into the public domain.

4.4 E-mail messages may be disclosed in legal proceedings in the same way as paper documents. Deletion from a user's inbox or archives does not mean that an e-mail cannot be recovered for the purposes of disclosure. All e-mail messages should be treated as potentially retrievable, either from the main server or using specialist software.

4.5 In general, staff should not:

4.5.1 Send or forward private e-mails at work which they would not want a third party to read;

4.5.2 Send or forward chain mail, junk mail, cartoons, jokes or gossip;

4.5.3 Contribute to system congestion by sending trivial messages or unnecessarily copying or forwarding e-mails to those who do not have a real need to receive them;

4.5.4 Sell or advertise using our communication systems or broadcast messages about lost property, sponsorship or charitable appeals;

4.5.5 Agree to terms, enter into contractual commitments or make representations by e-mail unless appropriate authority has been obtained. A name typed at the end of an e-mail is a signature in the same way as a name written at the end of a letter;

4.5.6 Download or e-mail text, music and other content on the internet subject to copyright protection, unless it is clear that the owner of such works allows this;

4.5.7 Send messages from another person's e-mail address (unless authorised) or under an assumed name; or

4.5.8 Send confidential messages via e-mail or the internet, or by other means of external communication which are known not to be secure.

5 USING THE INTERNET

5.1 Staff should not access any web page or download any image, document or other file from the internet which could be regarded as illegal, offensive, in bad taste or immoral. Even web content 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 the School's 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.

5.2 Staff should not under any circumstances use the School's systems to participate in any internet chat room, post messages on any internet message board or set up or log text or information on a blog or wiki, even in their own time.

5.3 The following must never be accessed from the network: online radio, audio and video streaming, instant messaging and webmail (such as Hotmail or Yahoo) and social networking sites (such as Facebook, Google+, Instagram, YouTube, Twitter). This list may be modified from time to time.

6 SOCIAL MEDIA

6.1 Staff must avoid making any social media communications that could damage the School's interests or reputation, even indirectly.

6.2 Staff must not use social media to defame or disparage the School, its staff or any third party; to harass, bully or unlawfully discriminate against staff or third parties; to make false or misleading statements; or to impersonate colleagues or third parties.

6.3 Staff must not express opinions on the School's behalf via social media, unless expressly authorised to do so by their line manager. Staff may be required to undergo training in order to obtain such authorisation.

6.4 Staff must not post comments about sensitive School-related topics, such as the School's performance, confidential information and intellectual property. Staff must not include the School's logos or other trademarks in any social media posting or in their profile on any social media.

6.5 The contact details of individuals made during the course of employment are the School's confidential information. On termination of employment staff must provide the School with a copy of all such information, delete all such information from their personal social networking accounts and destroy any further copies of such information that they may have.

6.6 Any misuse of social media, including content which disparages or reflects poorly on the School, should be reported to the Head Teacher.

6.7 Staff should make it clear in social media postings, or in their personal profile, that they are speaking on their own behalf. Write in the first person and use a personal e-mail address.

6.8 If a member if staff discloses their affiliation with the School on their profile or in any social media postings, they must state that their views do not represent those of the School. All staff should also ensure that their profile and any content they post is consistent with the professional image they present to pupils, parents and colleagues.

6.9 Staff may be required to remove any social media content that the School considers to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action

7 PERSONAL USE OF OUR SYSTEMS

7.1 The School permits the incidental use of internet, e-mail and telephone systems to send personal e-mail, browse the internet and make personal telephone calls subject to certain conditions set out below. Personal use is a privilege and not a right. It must not be overused or abused. The School may withdraw permission for it at any time or restrict access at its discretion.

7.2 Personal use must meet the following conditions:

7.2.1 Use must be minimal and take place substantially out of normal working hours;

7.2.2 Personal e-mails must be labelled "personal" in the subject header;

7.2.3 Use must not interfere with School commitments; and

7.2.4 Use must not commit the School to any marginal costs.

7.3 Staff should be aware that personal use of the School's systems may be monitored and, where breaches of this policy are found, action may be taken under the Disciplinary Policy. The School reserves the right to restrict or prevent access to certain telephone numbers or internet sites if it considers personal use to be excessive.

8 MONITORING

8.1 The School's systems enable it to monitor telephone, e-mail, voicemail, internet and other communications. For business reasons, and in order to carry out legal obligations in its role as an employer, use of the School's systems including the telephone and computer systems, and any personal use of them, may be continually monitored by automated software or otherwise. Monitoring is only carried out to the extent permitted or as required by law and as necessary and justifiable for business purposes.

8.2 The School reserves 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 business, including for the following purposes (this list is not exhaustive):

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

8.2.2 To find lost messages or to retrieve messages lost due to computer failure;

8.2.3 To assist in the investigation of alleged wrongdoing; or

8.2.4 To comply with any legal obligation

9 PROHIBITED USE OF THE SCHOOL'S SYSTEMS

9.1 Misuse or excessive personal use of the School's telephone or e-mail system or inappropriate internet use will be dealt with under our Disciplinary Policy. Misuse of the internet can in some circumstances be a criminal offence. In particular, misuse of the e-mail system or inappropriate use of the internet by participating in online gambling or chain letters or by creating, viewing, accessing, transmitting or downloading any of the following material will usually amount to gross misconduct (this list is not exhaustive):

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

9.1.2 Offensive, obscene, or criminal material or material which is liable to cause embarrassment to the School;

9.1.3 A false and defamatory statement about any person or organisation;

9.1.4 Material which is discriminatory, offensive, derogatory or may cause embarrassment to others (including material which breaches our Equal Opportunities Policy);

9.1.5 Confidential information about the School or any of its staff or students;

9.1.6 Any other statement which is likely to create any criminal or civil liability; or

9.1.7 Material in breach of copyright

Any such action will be treated very seriously and is likely to result in summary dismissal.

9.2 Where evidence of misuse is found the School may undertake a more detailed investigation in accordance with its Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or managers involved in the Disciplinary Policy. If necessary, such information may be handed to the police in connection with a criminal investigation.

Approval by Governing Body and Review Date

This policy and plan has been formally approved and adopted by the Local Governing Body at a formally convened meeting.

Signed: 

Chair of Governing Body

Date: 3 July 2017

Review Date: 3 July 2018

End of Statement