ELECTRONIC COMMUNICATIONS IN THE WORKPLACE ACCEPTABLE USE POLICIES (AUPs) AND GUIDANCE FOR STAFF, PARENTS and VISITORS

Status	Non Statutory Policy and Guidance (POLB)
Policy Written	April 2016 GK Checked by Michelmores
Policy Agreed	April 2016
Panel Responsible:	MAT BOARD BS AB
Origin:	Other MAT Model
Date Full Review:	April 2018
Policy Management:	CEO

ELECTRONIC COMMUNICATIONS IN THE WORKPLACE; ACCEPTABLE USE POLICIES (AUPs) AND GUIDANCE FOR STAFF, PUPILS, PARENTS and VISITORS

1 Introduction

For the purposes of this policy:

- where the word 'staff' is used, please assume this relates to staff and Directors/Governors.
- Where the word 'academy' is used, please assume all academies in the Trust and the Trust as a whole.

ICT is used by pupils of all ages, by teachers and by managers, and is an essential educational resource. Home Internet, apps and email use is now an important part of learning and communication during leisure time. However, as the Internet is managed by a worldwide collaboration of independent agencies, access to unsuitable materials is possible, security of computer systems may be compromised, and the e-safety of users may be at risk. This is a particular issue for academies, as we have a responsibility to our pupils and staff with respect to ICT, and in particular, to the use of the Internet. Staff and pupils also have a responsibility to use academy equipment carefully and to protect themselves when using ICT through academy provided equipment.

Risks associated with staff members' and pupils' use of the Internet, apps and e-mail include:

- Unwanted interactions, for example,
- staff members and pupils being targeted with racist or bullying e-mails;
- falsification, for example, the creation of e-mails which purport to come from a third party;
- Illegal use, for example, a staff member or pupil using the academy system to run an e-commerce business or to hack into other computer systems;
- Inappropriate access, for example, staff members or pupils accessing inappropriate materials, including pornography.
- System security, for example, files containing electronic viruses.

Staff should also carefully consider online safety in line with their safeguarding training and the guidance contained in Keeping Children Safe In Education. The following Acceptable Use Policies (AUPs) have been agreed to ensure that the academy's responsibilities to pupils, parents and staff are met. These AUPs are included as part of the academy's computing policy, and they relate to other policies, in particular that for behaviour and for personal, social and health education (PSHCE). The AUPs have been put in place by St Christopher's Multi Academy Trust (The MAT) to support schools and provide guidance in this important area of communication. It is suggested that each academy circulates this policy / displays it on the individual academy website.

2 AUP for staff

This AUP is designed to protect academy staff from harassment, real or alleged misuse and any consequential disciplinary action arising from the use of electronic communication equipment associated with academy. It is also intended to ensure that the academy's equipment is used responsibly and safely at all times.
Electronic communications equipment includes telephone, fax, voicemail, computer, laptops, apps, email, Internet, social networking sites, mobile phone, photocopier, digital cameras, videos and palm-held equipment. While the use of this equipment for academy business must come first, the academy allows employees to use this equipment for appropriate and moderate personal use. We trust employees to behave sensibly and to use equipment for personal use outside recorded working time (for example, at lunchtime).

Failure to follow any aspect of this policy (either deliberately or accidentally) could lead to disciplinary action in accordance with the academy's disciplinary policy, which may result in dismissal.

2.1 Safe and responsible use

2.1.1 The academy system

The computer system is owned by the academy and is made available to pupils to further their education and by staff to enhance their professional activities, including teaching, training, research, administration and management.

The Principal/Headteacher, Business Manager (BM) or Senior Administrator if no BM, or IT Manager, may examine and delete any files that are held on the academy system.

Academy computers are password protected.

Staff have access to an individual drive and a shared drive on the academy network. Staff must not wilfully make changes to computer settings, delete software or interfere with another person's files.

Staff are responsible for any academy equipment taken off site, for both its security and use whilst in their care. Where, for example, a digital or video camera is on loan, employees are responsible for removing all personal data.

Limited personal use of academy computers is acceptable outside working hours.

Phone calls, faxes, photocopying, printing for personal use are acceptable, provided they are paid for.

When unattended, computers holding personal information should be logged off or locked. All documents containing personal data must be password protected.

All laptops must be encrypted.

In communications with pupils and parents, staff must never give out personal information which identifies their home address, phone number, mobile phone number or personal email address.

Staff must never use their own personal communications device, such as a mobile phone or personal email to communicate with pupils or parents. There have been a number of cases of parents and pupils bullying teachers in this way. Staff must not use

their personal email to communicate with parents: contact must bemade via the office accounts..

2.1.2 The Internet

The Academy provides a filtered Internet access, some of the MAT's schools also have and a safe virtual learning platform for electronic communication with pupils.

Reasonable personal use is permitted outside of recorded working time (for example, at lunchtime).

Internet sites accessed may be monitored by the Principal/Headteacher, office or ICT technicians.

2.1.3 E-mail

The academy provides all members of staff with an academy email account for all work-related communications. It is not to be used to store or circulate personal emails. Emails are a means of formal communication and as such must be written in a professional tone and text. The use of obscene language or swear words is strictly prohibited.

Be aware that: emails may be submitted as evidence in legal proceedings. email discussions with third parties can constitute a legally binding contract. Email is governed by the same rules which cover all home-academy correspondence. Therefore, copies are kept as a record of the communication, for example, by keeping a printed copy, or forwarding the email to the academy office or other relevant staff.

Staff do not access the email of other individuals within the academy without express permission and a clear understanding of the reason for the proxy access.

Academy email accounts may be accessed by the Principal/Headteacher, administration team, office staff or IT Manager.
Staff must not open email attachments unless they have absolute confidence in their origins. This is one of the most likely points of access of a virus into the academy's computer systems.

It is impossible to control what information is sent to a member of staff by email. If offensive, obscene and/or discriminatory material is received, it is the responsibility of the receiver to report it immediately to the Principal/Headteacher.

2.1.4 Web logs (blogging) and social networking sites

It is recognised that a number of online communications tools, such as blogs, have a potentially useful role in schools. Blogs and all such communications must contain a disclaimer that the views expressed are personal and not necessarily those of the academy or St Christopher's Multi Academy Trust.

Any meeting or correspondence between staff and parents that originates through the school/MAT should be part of a professional, not social, relationship. There is a fine line between the relationships established with colleagues and other people associated with academy (including parents) through social networking and it is highly recommended that staff do not make links with parents on social networking sites, as staff using social networking sites could be seriously at risk from harassment and invasion of privacy, particularly if they can be identified from their login names. Staff must not, under any account make links with pupils on social networking sites. This will be regarded as a safeguarding issue and will be dealt with through the Disciplinary Policy.

Pictures / videos taken at the academy must not be loaded onto personal social networking sites.
Pictures of staff taken outside the academy may be uploaded with their permission, so long as the academy is not identified. Personal pictures / texts must not identify the academy. The content of any personal social networking site must not discuss academy business or personnel, be this directly or indirectly through implication.

2.1.5 A IT equipment provided by the academy

- Ownership of IT equipment rests with the academy.
- Staff have full use of the IT equipment to support their work in the academy..
- Staff can only install approved (by the headteacher) software or apps on the laptops/Ipad, and the headteacher must be satisfied that all licence requirements are met.
- Headteachers, together with the Business Manager may choose their own Internet Service Provider, and are responsible for any charges incurred.
- Staff are reminded that they should, under no circumstances, deliberately seek out pornographic, inappropriate or offensive materials on the Internet, and that they are subject to criminal legislation and disciplinary procedures should they do so.
- Anti-virus software is installed on the laptop, and staff are responsible for ensuring that this is kept up-to-date. Staff may not change the Anti-virus software without expressed permission from the Principal/headteacher
- Staff must password-protect the laptop / Ipad/PC and the academy will keep a copy of the passwords.
- All documents holding personal data must be password protected
- Individual Academies will have their own procedures for ensuring data is secure by making regular backups of files on the laptop/Ipad/PC and encrypting devices; if staff carry this out personally they must ensure that backups are kept safe and secure.

2.1.6 Mobile phones

- Staff may share personal mobile numbers with other staff.
- Staff should not share personal mobile numbers with parents
- Staff must not phone, take photos or text pupils using personal mobile phones
- Staff must keep personal mobile phones securely when on site and should carry them in bags or pockets whilst entering or leaving the premises.
- Staff must not use mobile phones whilst entering or leaving the premises during academy hours.
- Staff must not use mobile phones during teaching time unless there is an emergency.
- Where personal mobile phones are used to access their academy email account the email must be password protected and the mobile must have secure PIN access. No material containing personal data of any student, parent or staff must be downloaded onto any personal device.
- They are primarily taken where the risk to safety outweighs e-safety concerns and should only be used to contact the academy, staff or emergency services.
- Mobile phones may be required for safety reasons in off-site activities; an academy mobile phone may be provided for contact with the academy. Staff may be required to use personal mobile phones in an emergency situation if off site. Staff may need to take their mobile phones for safety reasons: but these should not be used to contact parents unless there is an emergency situation. They must not be used to contact pupils.

2.1.7 Cameras, photographs and videos

- The school may provide classes with digital cameras for use by staff and pupils.
- Staff must not take an academy camera home even in connection with academy work; any stored photos must not be transferred onto personal devices.
- Pictures must be stored on the academy server.
- Use of pictures follows the academy policy with regard to parental permission.
- Staff must not use personal cameras to take photos of pupils.
- Uploading staff photographs onto social networking sites follows the guidelines above.
- Parents may video academy productions, with permission from the principal/headteacher but these must not be uploaded onto the Internet.

2.1.8 The academy website

- The academy maintains editorial responsibility for any academy-initiated web site to ensure that content is accurate and quality of presentation is maintained.
- The academy maintains the integrity of the academy web site by ensuring that responsibility for uploading material is never handed over to pupils.
- The web site complies with the academy's guidelines for publications.
- All material must be either the author's own work, or must state the author's identity or status, and must not break copyright.
- The point of contact on the web site will be the academy address, e-mail and telephone number. Home information or individuals' personal e-mail addresses must never be published.
- The academy obtains permission from parents for the use of pupils' photographs. Photographs do not have a name list attached. Identities of pupils must be protected at all times.
- Staff personal photos must not be uploaded onto the academy website.

2.1.9 Mobile data storage (memory sticks)

- By far the most common case of data-confidentiality breaches come from memory stick losses, together with bringing virus' in to the system. Memory sticks are not to be used under any circumstances Encrypted hard drives can be used but only where there is virus protection software installed and they are not also used with personal devices.
  Pupils must not bring memory sticks to the academy.

2.1.10 Misuse of electronic equipment

- Misuse is a serious disciplinary offence.
- Employees MUST NOT use the academy equipment at any time to:
  - store, view, download or distribute material that is obscene, offensive or pornographic, contains violent images, or incites criminal behaviour or racial hatred;
  - gamble using academy 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);

- send emails or publish anything on a website or blog, which:
    - are critical about members of the academy community including pupils,
    - contain specific or implied comments you would not say in person,
    - contain inappropriate comments which could cause offence or harassment on the grounds of gender, race, disability, age, religion or sexual orientation;
- have originated from a chain letter;
- conduct private and intimate relationships via email;
- download or copy software (excluding software updates) onto academy equipment or use the email system to transmit any documents or software without checking copyright or licence agreement;
- install software licensed to the academy on a personal computer at home unless permission to do so is explicitly covered by the academy licence agreement;
- do anything which brings the academy or St Christopher's Multi Academy Trust into disrepute.

2.2 Acceptable Use Policy for pupils

Staff must be familiar with the Academy's AUP for pupils. Refer to section 3
Staff supervising Internet and email use must be given appropriate training.

2.3 Monitoring and privacy

The academy's email and Internet facilities are business systems, owned by the organisation. The academy therefore reserves the right to track all use of the Internet and of the academy's IT systems. Usage may 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. The Headteacher, administration team and IT Technician have proxy access to all the academy'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 academy's network or being circulated via the academy'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.

2.4 Breaches and sanctions

Failure to follow any aspect of this policy, either deliberately or accidentally, could lead to disciplinary action in accordance with the academy's disciplinary policy which may result in dismissal.

3 AUP FOR PUPILS

3.1 Introduction

The AUP for pupils is discussed each year with pupils and their agreement to its rules is obtained by pupils signing the ICT Contract.

3.2 Safe and responsible use

3.2.1The academy system

- Pupils sign the ICT Contract at the beginning of each year to agree to follow rules concerning safety and responsibilities about using ICT in academy.
- Pupils from Year 1 have a personal log in.
- Pupils access their own files and must not access other people's files.
- Pupils must treat equipment with care.
- Pupils must not download software or games.
- Pupils must not print without permission.
- Pupils in KS2 & KS1may log in at lunchtimes to access a limited choice of activities, under the supervision of an adult.
- Failure to comply may result in sanctions: see below.

3.2.2 The Internet

- Pupils have access to a filtered Internet source to support learning.
- Pupils must ask permission before accessing the Internet.
- In KS1, pupils access only sites approved by an adult and an adult always monitors Internet use.
- In KS2, pupils access a wider range of sites and an adult is always present.
- Pupils must not access personal chat rooms.
- If pupils access inappropriate sites by accident, they must tell an adult
- Pupils are taught to be aware that at some point, they are likely to access inappropriate sites by accident, and they must tell an adult.
- If pupils deliberately access inappropriate sites, sanctions will apply: see below.
- Pupils are aware that their Internet usage is monitored by staff.
- Pupils must not enter personal data onto the Internet.

3.2.3 Email

- From Year 1 pupils may have access to a safe email account.
- Pupils may email to addresses of approved recipients only. Usually, the academy system is set up so that pupils are unable to email outside academy. At occasional times, settings can be altered by staff to allow emails outside academy to specified addresses. Pupils have no email access that allows them unrestricted addressees.
- Pupils must keep messages polite.
- Pupils are aware that emails are monitored by staff.
- If pupils receive emails that they find upsetting, they know to tell an adult.
- If pupils receive an email from an unknown source, they know not to open the email, and they must tell an adult.
- Failure to comply may result in sanctions: see below.

3.2.4 Blogs, forums and social networking sites

- Pupils may access these as directed by staff for learning purposes.
- Pupils must keep postings polite.
- Pupils must not access personal social networking sites at the academy.

- Pupils must not make requests to create links with staff on social networking sites.

3.2.5 Laptops/IPads/PC's

Pupils must take care when using academy laptops, IPads and PC's, maintaining an awareness of their fragility. All such devices should be fitted with a protected cover where appropriate.

3.2.6 Mobile phones

Pupils are not to use mobile phones in school. If they do bring mobile phones to school for safety reasons (e.g. Y6 walking home alone) they must be handed in at the start of the school day; parents must understand that if their children bring their phone into school this must be at their own risk and this must be made clear in the consents booklet..

3.2.7 Cameras and photographs

Pupils have access to academy digital cameras which they may use with permission from an adult.

Pupils' parents sign to agree / disagree to photos of pupils being used on the academy website and in newspapers.

Pupils' must not upload pictures of pupils or staff unless given permission.

3.2.8 The academy website

Pupils may access the academy website and are encouraged to contribute to its content; but they may not upload personally.

3.2.9 Virtual Learning Platform

Pupils may have individual access to a Virtual Learning Platform. They may access this at the academy and at home.

Pupils may have a personal home page on the VLE which they may modify. Pupils are responsible for the content of this homepage and it must be polite. Pupils must not include personal information on their homepage.

3.3 Sanctions

Pupils are aware that if they break rules concerning ICT use, they will be stopped from using school's ICT equipment.

Instances of cyber bullying are dealt with in accordance with the academy's Anti-bullying Policy.

4 AUP for PARENTS AND VISITORS

4.1 Mobile phones

The academy recognises that people may wish to have their personal mobile phones with them to use in case of emergency.

However it is also recognised that personal mobile phones have the potential to be used inappropriately and to safeguard our children we request all parents and visitors comply with our personal mobile phone policy.

- Mobile phones and cameras should only be used in the office reception area or off site.
- In very unusual circumstances, such as a family emergency, parents & visitors should seek permission from the supervising member of staff/SLT to use their mobile phone on the school's premises.
- If parents & visitors need to be contacted they should request that the academy's landline number is used. A member of staff will then contact them.
- Photos of children must not be taken without prior discussion with the headteacher and in accordance with the Data Protection Act 1998 (please refer to the setting document 'Guidance for settings on the use of Images, Mobile Phones and Cameras').

In circumstances where there is a suspicion that the material on a mobile phone may be unsuitable and provide evidence relating to a criminal offence the 'Allegations regarding Person(s) working in or on behalf of Academy (including Volunteers)' process under the Academy's Safeguarding Policy will be followed.

Parents and visitors remain responsible for their own property and will bear the responsibility for any losses

Appendix I gives an explanation of the classifications used when investigating electronic communications misuse and is used as a guide. There may be material that does not readily fit into these categories.

Appendix II details the factors that are considered before deciding the appropriate sanction in cases of electronic communications misuse.

Appendix I: Classification of Electronic Communications Misuse *TERM*	*MEANING*	*RATING*	*SANCTION*
Gross	*Time* *Volume* *Capacity* *Offensive material of the following nature: sexually explicit or suggestive, usually in picture format; racist homophobic; ridiculing religion, disability, sexual orientation or politics; ridiculing/demeaning individuals; inciting cruelty or illegal activity* *Material intended for the purpose of radicalisation*	*Gross Misconduct*	*Dismissal*
Serious	*Time* *Volume* *Capacity* *Offensive material of the following nature: sexually orientated; bad and offensive language; politically aggravating; ageism; showing violence or nudity*	*Serious Misconduct/ Misconduct*	*Final written warning / written warning*
Mild and Non-offensive	*Time* *Volume* *Capacity* *Material of the following nature: jokes/short stories with minor references to material of a sexist nature or in bad taste; jokes/stories etc. of a non-offensive nature (that is, not gross, serious or mild); light hearted material; cute animal pictures*	*Misconduct*	*Written warning / verbal warning / informal process*

Capacity – *material that takes up a lot of capacity on the hard drive of the email account*
Time – *personal use could be considered tantamount to fraud*
Volume – *the numbers being received and/or sent on*

Appendix II: Factors to take into consideration before deciding the appropriate sanction in cases of email and Internet abuse

If the allegations are proven, then consideration should be given to whether they are gross misconduct or other misconduct. Gross misconduct can be defined as misconduct for which dismissal would be appropriate without previous warnings. If the misconduct is not gross, then dismissal would not normally be appropriate without previous warnings. Before reaching a decision on the appropriate sanction, the following factors should also be taken into account:

1. Seniority: has the manager failed to set an example to the team? Has the manager challenged inappropriate behaviour amongst the team being managed?

2. Realisation of Misconduct: has the employee understood the implications of the breach of discipline?

3. Behaviour Change: is the employee likely to repeat the misconduct, or is a desired change in behaviour likely?

4. Coercion: did the employee feel pressure to join in these activities, either through their peers or, more worryingly, their manager?

5. Instigator: is the employee at the heart of the email abuse, encouraging and/or promoting the distribution of material?

6. Recipients

7. Policies breached

8. Environment: have the images been viewed in an area where pupils, service users or members of the public might be able to see it?

9. External Contact: has material been exchanged with those outside the organisation which would increase the risk of reputation of the academy being d

POLICY CONTROL DETAILS

Date	Page	Details of Change	Agreed by: