The St Marylebone CE Bridge School

A Special Free School for pupils with Speech, Language and Communication Needs

Herries Street, London W10 4LE

ICT Acceptable Use Policy (Staff)
(including Staff Social Networking and Email Policies)

Committee:	**Governing Body**
Author:	**Kate Miller**
Last reviewed:	**July 2023**
Review cycle:	**Annually**
Required to publish on website?	**No**
Statutory:	**No**

1. Context

1.1 The aim of this policy is to set out safe and responsible behaviour when using ICT facilities at The St Marylebone CE Bridge School ("the School"). These facilities include computers, laptops, iPads, mobile devices, peripherals, software, email, Google Drive, the managed learning environment and internet access, both onsite and off-site.

1.2 The School recognises and embraces the potential of ICT to enhance teaching and learning. ICT equipment and services are provided in order to support the school community and make sure that everyone has access to the benefits of technology.

1.3 The School's networked ICT facilities serve as a first line of defence in keeping users safe and secure. We use a range of security techniques for this, including anti-virus software, internet filtering and email and network monitoring. Our managed service provider monitors all network use and can report back detailed information about each user's activity on the network.

1.4 As an overall principle, all staff are advised to use all ICT and internet-based communication with caution and full awareness of the potential impact of their online activity on their professional life, the safety of students, their own safety and reputation and the reputation of the School. All staff are responsible for safeguarding; this relates to managing their own conduct as well as responsibly reporting the inappropriate conduct or misconduct of others.

1.5 It is important that all staff take responsibility for their own use of ICT and internet-based communication, making sure that they behave safely, responsibly and legally. The School will treat any breach of policy very seriously.

1.6 This policy should be read in conjunction with the School's Data Protection Policy and Data Protection Code of Practice including email security.

2. Expectations of staff

2.1 All staff are expected to:

2.1.1 Stop and think before clicking, so that sound professional judgements are made about what is communicated, found, used and shared.

2.1.2 Be aware of their social and professional responsibilities when using ICT and with regard to all online activity.

2.1.3 Report any misuse of ICT or online activity, including unprofessional conduct or bullying, to their SLT line manager or, in the absence of the line-manager, to the Deputy Head of School or Head of School.

2.1.4 Ensure that their online activity and use of ICT, whether at school or outside, does not bring the School or any of its community into disrepute.

2.1.5 Take steps to safeguard their own online profile or profiles on social networking sites to ensure that these cannot be seen by students or parents.

2.1.6 Respect the technical safeguards that are in place. Trying to breach technical safeguards, conceal network identities, or gain unauthorised access to systems and services, is unacceptable.

2.1.7 Report any failings in technical safeguards.

2.1.8 Protect their password and personal network login and not share this with others inside or beyond the school community.

2.1.9 Log off the network when leaving computers unattended.

2.1.10 Access only the resources which they have permission to access. Any attempts to access, corrupt or destroy other users' data, or compromise the privacy of others in any way, using any technology, is unacceptable.

2.1.11 Protect the security and confidentiality of school data and networks at all times and take care when transferring files and opening attachments in order to avoid introducing viruses or inappropriate material into the school (see further guidance below).

2.1.12 Use only the School email system for School-related email to ensure safety and security (see further guidance below).

2.1.13 Print responsibly in order to reduce costs and minimise wastage.

2.1.14 Be aware of intellectual property and copyright: staff are reminded that even accidental plagiarism may qualify as an illegal infringement of copyright and a criminal offence.

3. Specific guidance regarding online materials, photographs and the use of inappropriate materials

3.1 Where new technology, audio-visual media or film resources are used as part of teaching and learning or student support, staff are advised always to ensure that the resource is clearly linked to the learning, is age appropriate and ensure that it complies with UK ratings restrictions and the School's own internet filtering systems. In the rare case in which a resource does not meet these criteria, the resource can be used only with approval from the Head of School. If in any doubt about the appropriate nature of material, the SLT line-manager for the subject must be consulted. It might be deemed appropriate or necessary to gain parental consent.

3.2 Staff are advised to always check websites in advance before giving web addresses to students. This includes checking that a source is trusted and reliable.

3.3 Any publication of pictures of students in School publicity should ensure their privacy, dignity and security at all times. Students whose parents have expressed the wish for them not to appear in photographs must not be photographed, as per the Home-School Agreement. Photographs of students should not be used for any purpose other than School purposes.

3.4 Staff must not possess any indecent images of any young people. Breach of this is likely to be considered as gross misconduct.

3.5 Staff must not access pornography or any other material which is illegal or inappropriate to the School environment while in School or off-site in a professional capacity, on any ICT device. Breach of this is likely to be considered as gross misconduct.

3.6 Staff must not use equipment belonging to the School to access pornography or any other material which is illegal or inappropriate to the school environment. Equipment containing such material should not be brought on to school premises. Breach of this is likely to be considered as gross misconduct.

4. Specific guidance regarding Email Communication

Although the School recognises that e-mail is a useful form of communication, there is a danger that staff can be overloaded by huge volumes of e-mails, many of which may not be relevant to them. In order to reduce the amount of e-mail delivered to our inboxes, staff are requested to consider if the e-mail they are about to send is really necessary. Would a conversation or a phone call be more efficient or more appropriate? In addition, there are issues of **safeguarding and security** for all e-mail users, and all staff need to be mindful of these. Staff must use the School email system when emailing students and parents.

4. 1. Addresses

4.1.1 Staff should always use their professional school E-mail address when communicating on School matters. This includes communication to colleagues, students, carers and other external agencies.

4.1.2 The following applies when there is more than one recipient:

i. All user groups should be **bcc** not cc or "to".
ii. All recipients should be **bcc** not cc.
iii. External recipients, including parents/carers should be **bcc**.
iv. Be careful to select the correct recipients both when you send and reply.

4.1.3 "4.1.2" does not apply when it is professionally necessary to make all recipients aware of who has received the e-mail, and who may respond.

4.2. Subject line

To help recipients identify the type of email please use the following titles in subject lines and in general **Whenever possible please e-mail individuals and specific groups rather than everybody.**

4.2.1 **SPAM: Use this when addressing groups of staff about matters of interest to them but not relating to work.**

4.3 Content

4.3.1 Staff are advised to ensure that all email communication is transparent, professional and does not promote or imply (however unintentionally) inappropriate relationships between staff and students or parents.

4.3.2 Staff are advised always to check the content of all electronic communication and ensure that it is addressed to the appropriate person.

4.3.4 The School email system is monitored using remote checking. This can be used to check the appropriateness of messages sent and received.

4.3.5 Communication between students and staff should take place within clear and professional boundaries so as to avoid any possible misinterpretation of motives or behaviour which could be construed as grooming or favouritism by the student, their family, other staff or members of the School community or public. This includes the use of mobile phones, text messaging, emails, digital cameras, videos, webcams, websites, blogs, applications and social networking sites.

5. Specific guidance with regard to social networking

5.1 Everyone at the School has a responsibility to ensure that they protect the reputation of the School, and to treat colleagues and members of the School with professionalism and respect.

5.1.1 This policy relates to social networking outside work.

5.1.2 It is important to protect everyone at the School from allegations and misinterpretations which can arise from the use of social networking sites.

5.1.3 Safeguarding children is a key responsibility of all members of staff and it is essential that everyone at the School considers this and acts responsibly if they are using social networking sites out of School. Anyone working in the School either as a paid employee or volunteer must not communicate with students via social networking.

5.1.4 No communications irrespective of their anonymity should be shared that relate to any specific event, protocol, student or person at the School.

5.2. Code of Conduct for Everyone at the School – Social Networking

The following are **not considered acceptable**:

5.2.1 The use of the School's name, logo, or any other published material without written prior permission from the Head of School. This applies to any published material including the internet or written documentation.

5.2.2 The posting of any communication or images which link the School to any form of illegal conduct or which may damage the reputation of the School; this includes defamatory comments.

5.2.3 The disclosure of confidential or business-sensitive information or the disclosure of information or images that could compromise the security of the School.

5.2.4 The posting of any images of employees, students, trustees or anyone directly connected with the School whilE engaged in School activities.

5.3. In addition to the above everyone must ensure that they:

5.3.1 Use social networking sites responsibly and ensure that neither their personal/professional reputation, nor the School's reputation is compromised by inappropriate postings.

5.3.2 Are aware of the potential for their personal social networking pages to be seen by students and parents and so ensure that all security settings are set so that their pages are not open to public view.

5.3.3 Do not access blogging and social networking sites at work, using School equipment.

5.4Prior to joining the School, new employees should check any information they have previously placed on social media sites and remove any statements that might cause embarrassment or offence

5.5 Potential and Actual Breaches of the Code of Conduct:

In instances where there has been a breach of the above Code of Conduct, the following will apply:

5.5.1 Any breaches of this policy will be fully investigated. Where it is found that there has been a breach of the policy this may result in action being taken under the School's Disciplinary Procedure.

5.5.2 The Governing body will take appropriate action in order to protect the School's reputation and that of its staff, parents, trustees, students and anyone else directly linked to the School.

6. Sanctions

6.1 This policy relates to all members of Staff. As such, all staff are expected to report inappropriate conduct or suspected inappropriate conduct to their line-manager or, in the absence of the line-manager, the Deputy Head of School or Head of School.

6.2 Breaches of this policy will be dealt with according to the School's Safeguarding and Child Protection Policy and / or The School's Disciplinary Procedures as appropriate.

6.3 Any illegal use of the School's ICT facilities, inappropriate conduct or activity which compromises the safety and / or well-being of students, will be reported to the police and/or relevant child protection agencies. In such instances, the School will follow its Safeguarding and Child Protection Policy and / or disciplinary procedures as appropriate.

6.4 Where unacceptable use is suspected, by a member of staff, enhanced monitoring and reporting procedures may come into action, including the power to check and/or confiscate personal technologies such as mobile phones.

7. This policy should be read with reference to

The Data Protection Code of Practice
The Data Protection Policy
The School's Disciplinary Procedures
The E-safety Policy
The Safeguarding and Child Protection Policy
The Staff Code of Conduct

When implementing this policy the latest guidance will be referred to, even if the guidance has changed since the last policy review.