WILSON'S SCHOOL

ACCEPTABLE USE POLICY

(including Use of Email Policy)

Date approved by governors: March 2022

Date for Review: March 2025

Wilson's School provides computers for use by staff and students for employment and educational purposes. This equipment is provided and maintained for the benefit of all. This policy is designed to ensure that the equipment and facilities are used and cared for by users in an appropriate manner. **Where applicable, these provisions also apply when staff and students are using privately owned devices for school work or when on school premises, including through the use of their own networks or other internet connections.**

Equipment

Users must:

- Always check files brought in on removable media (such as CDs, flash drives etc.) with antivirus software and only use them if they are found to be clean of viruses. Changes to the set-up and configuration of computer equipment may only be carried out by IT Support staff.
- Always check that mobile equipment (e.g. laptops, tablet PCs, PDAs etc.) has antivirus software and ensure that it has been found to be clean of viruses before connecting them to the wireless network. Users must not damage, disable, or otherwise harm the operation of computer hardware.
- Ensure that portable IT equipment such as laptops, digital still and video cameras are securely locked away when they are not being used. Users must
- Report any problems with the equipment or systems to IT Support as soon as practicable. Users must not connect any device not owned by Wilson's School and looked after by IT Support to the school's wired network.

Users must not:

- Eat or drink in a computer room or near IT equipment in order to protect computers and other equipment from.
- Remove labels from computers or other computer equipment.
- Remove any equipment from the premises (including cameras and video cameras) without signing it out in the IT loans book.

Safety, Security and Privacy

Users must:

- Keep passwords secret; never use someone else's logon name or password. They must never allow anyone else to use their username or password.
- Select a strong password when establishing a logon to any internet site or service, ensuring the password is at least eight characters, consisting of a random mixture of upper and lower case alphabetical and numerical characters.
- Ensure that passwords are changed at least every term, or as soon as there is a suspicion the password may have become known. In these circumstances, users must change their password immediately and report the matter to the IT Support Department and the DPO if there is suspicion that logon details have been compromised.
- Always be wary or seek advice before revealing personal details such as home address, telephone number, school name, or pictures to people via the Internet.
- Ensure that all logon details are safeguarded and details entered are not viewed by anyone else when using Remote Access. Keep these details safe, secure and secret. Consider the location used for remote access and ensure information cannot be

accessed by anyone else. Portable devices with access to the school account, including email, must be protected with a pass code which is kept safe, secure and secret.

- Only use school systems, including email, for the conduct, creation and storage of work related to the performance of their duties and legitimate educational and curriculum purposes.
- Always represent the school appropriately online, upholding its values and maintaining its reputation and must not undertake any activity that undermines the School or its community.
- Take reasonable care when using services, appreciating the ease at which information can easily be transmitted outside of the school's care and control, and the ease with which comments and views portrayed can be misinterpreted. It is far preferable to use hyperlinks to folders on the school system rather than attaching sensitive documents (or documents containing any personal data) to emails. Any such attachments must be password protected.
- Remain vigilant when opening email to protect against malicious content. Attachments can contain viruses or other programs that could destroy all the files and software on a computer; hyperlinks must also be treated with caution. If in doubt do not open the item and seek further advice.
- Ensure that any private social networking sites / blogs etc. are not confused with, or otherwise undermine, the school.
- Check, prior to use in a classroom setting, any live internet materials to ensure that the content of such materials (including any background banners and pop ups) is not in breach of any of the provisions of this policy.
- Observe the Use of Email Policy (see below).
- In the Sixth Form, be fully aware of and comply with the provisions of the Sixth Form Agreement which apply in addition to and in conjunction with this acceptable use policy.

Users must not:

- Enter into any legally binding or contract agreement on behalf of or while representing the school, via the internet alone, without authority to do so.
- Enter into or undertake any activity that could be classed as gaming or gambling.
- Access, exchange or present offensive, racial, defamatory, discriminatory, pornographic or obscene remarks, comments, material or language.
- Enter into any form of discrimination, bullying, victimisation or harassment.
- Enter into or undertake any activity that may be classed as illegal or unlawful.
- Enter into or undertake any activity that may breach any copyright or licence agreement.
- Impersonate any other person, through claims made, suggestion or the changing of logical settings (spoofing), or otherwise.
- Trespass into other users' files or folders.
- Utilise any means, mechanisms or tools to circumvent any school's internet control or restriction applied.
- Purchase, install, or download (without express prior permission) software or subscribe to or take part in any form of publicly available internet chat or discussion (via such means as Message Boards and Forums, Web Chat, social networking etc.), on behalf of

or while representing the school. Users must ensure that they are familiar with the Staff Conduct Policy with reference to the use of social networking sites.

Nothing in this policy prevents members of teaching staff from using, in the context of their legitimate teaching activity, materials which are racist, homophobic or otherwise offensive provided that this is with the clear intention of challenging the prejudices these materials embody.

Please read this document carefully. Violation of any of these provisions could lead to disciplinary action, including dismissal, and in some instances could lead to criminal prosecution or other legal action. Anyone under reasonable suspicion of misuse in terms of time, activity or content may be placed under retrospective investigation or have their usage monitored.

Use of Email Policy

This policy lays out expectations for the appropriate use of the school's email systems and for communication by email between stakeholders. Please read this policy in conjunction with the Acceptable Use Policy above.

The IT Support team is available to all staff in the school to explain how to use email software. Contact: itsupport@wilsonsschool.sutton.sch.uk.

Section 1: Safeguarding

The provisions in this section are professional expectations on all staff.

In order to ensure the safeguarding of students and protection of staff, the following guidelines must be followed:

a) All emails between individual staff and individual students must be copied to the member of staff's pastoral or academic line manager.

If the email concerns academic matters:

- Subject tutors Cc to Heads of Department.
- Heads of Department Cc to their line manager.

If the email concerns extra-curricular matters

- All staff Cc to Head of Year or a member of SLT

If the email concerns any other matter:

- Tutors Cc to Head of Year or Key Stage Director.
- Year Managers Cc to a member of SLT.
- Members of SLT Cc to the Head.

- Head Cc to appropriate member of SLT.
- Support staff Cc to most appropriate member of staff, except in very limited and specific circumstances such as password reset emails.

b) All contact between staff and students must be via the school email system. Staff must not accept emails from students' personal email addresses. (If a student sends you an email from a personal account you should return it with an indication that it can only be accepted via the school system. You should Cc your return to the appropriate member of staff.)

c) Staff must not give students their personal email addresses, any indication of their personal social media profiles, or any other personal contact details.

d) Ideally, SIMS InTouch (or other formal email communication tool) will be used for the purpose of communicating with groups of parents. When Outlook is used, care must be taken not to include the email addresses of other parents or members of staff. Where necessary the blind copy function should be used.

e) Outlook must never be displayed on white boards; the display of the desktop alert must be disabled.

The provisions in the following sections have the status of guidance.

Section 2: General expectations for use of email

a) There is no expectation that subject teachers will use email to communicate with students or parents. This is a matter of individual choice. However if an email is received from a parent, a short reply should be sent indicating contact details for an appropriate colleague (e.g. Head of Department or Director of Key Stage).
b) Members of staff may request a change of school email address. Changes will be implemented only at the beginning of a term.
   All members of staff are expected to check their school email account once per day on the days when they are in school and to read all messages sent to them by colleagues within 24 hours (see section 5b). All members of staff should be aware that some colleagues are part time, and cannot be expected to read or deal with email when they are not at work.
c) Check email recipients very carefully being wary of the auto-complete function to ensure that all communications are sent to the intended recipient.
d) Be aware when attaching documents containing personal data to email communications. Consider using hyperlinks or password protection to documents where relevant.

If you are concerned about the content or tone of an email that you have received, speak to the relevant Key Stage Director (in the case of an email from a student), your Head of Department or a member of SLT (in the case of an email from a parent, colleague or any other contact).

Section 3: Protocols for the use of email to communicate between staff and parents.

a) It may be appropriate to email parents to register concerns or praise for work, behaviour or wellbeing; it is usually best to Cc a Head of Department or Head of Year into such an email.
b) Remember your email is a communication from you as a professional. You should take sensible care with spelling and punctuation. Your email should contain a suitable salutation and sign off.
c) Emails to parents should be brief and to the point. Do not allow a disagreement with a parent to develop through a to and fro of email correspondence. If there is a significant disagreement, arrange a meeting to resolve it, engaging support from departmental or pastoral colleagues as appropriate.
d) Never write in anger an email to a parent about a student. Always allow a cooling off period. Consult with a colleague before emailing and get someone to check the text for tone. If you wish to complain about a student's work or behaviour, consider phoning instead. If you think that the content of your email may be in any way contentious, check with your line manager first and Cc him/her in.
e) Only if you know the parent very well should you think of using an informal tone. Emails between staff and parents should normally have a professional and reasonably formal register.
f) Emails to parents should be composed as carefully as letters. Emails containing information about a child's welfare should be transferred onto child protection management software (currently CPOMS).
g) Emails from parents can normally be treated as letters. NB: This does not apply when an email contains a confidentiality notice stating that it must not be printed or forwarded without the permission of the sender.
h) Do not give parents your personal email address or any other personal contact details.

Section 4: Protocols for the use of email to communicate between staff and students.

a) It is appropriate to email students <u>at their school email address only</u> to communicate about homework, missed work or other school related activity, such as participation in an extra-curricular activity.
b) Use a courteous and reasonably formal and professional tone. Avoid banter, sarcasm or jokes or anything that may be considered over-familiar.
c) Never discuss personal or confidential matters: theirs, yours or anyone else's.
d) Do not use email to discuss behavioural matters or to set detentions.
e) Never refer disparagingly to any person in an email to a student.

Section 5: Protocols for the use of email to communicate between colleagues at Wilson's

a) There is no expectation for colleagues to read their emails more than once per day. Therefore do not expect a response or action in response to your email in less than 24 hours.
b) If you need a colleague to act upon a message or be aware of information urgently (in less than 24 hours) do not use email to communicate the message unless you are sure your colleague checks his/her emails regularly. If so, flag the email as urgent.
c) Avoid sending emails to colleagues at weekends wherever possible. With regard to the 24 hour rule, an email sent on Friday evening or over the weekend should be considered to have been sent on Monday morning. If possible, use the 'delay delivery' option in Outlook.
d) Remember that your emails are not private. While they are not continuously monitored, they can be accessed with authorisation from the Head and/or Deputy Head in controlled circumstances. Maintain a professional tone and content in all school emails.
e) The use of remote access to school email accounts is entirely voluntary. There is no expectation that staff should access their emails from home.
f) If you need to forward an email to another colleague, consider whether you should seek permission to do so from the sender in advance.
g) E-mails should not be sent advertising services or items for sale.

Section 6: Protocols for the use of email to communicate with anyone else.

a) Members of staff are responsible for the content of their Outlook account, which must comply with all school policies regarding possession or distribution of indecent material and material liable to cause offence because of its discriminatory or prejudiced content. If a member of staff is worried that they have received something inappropriate, they should contact the IT Support team and delete the email promptly thereafter. Members of staff are also responsible for managing the content of their mailboxes and following any instructions given about the retention of email.
b) Maintain a professional tone and content in all emails sent from your school address.
c) To comply with Companies Act requirements, members of staff must ensure that any email sent outside of the school includes a sign off giving details of the school name, registered office and company registration number.