WILSON’S SCHOOL

ACCEPTABLE USE POLICY

Date approved by Trustees: Autumn 2025

Date for Review: Autumn 2027

Wilson's School provides IT equipment and services for use by staff, contractors, visitors and for employment and educational purposes. This Acceptable Use Policy outlines how we expect all members of the school community to behave when they are online, and/or using school networks, connections, internet connectivity and devices, cloud platforms, AI tools and social media (both when on school site and outside of school). Equipment/devices may include desktop computers, laptops, mobile phones, tablets, digital cameras, and email as well as IT networks, data and data storage, remote learning and online and offline communication technologies (this is not an exhaustive list). This policy also applies when adults and students are using privately owned devices for schoolwork, or when on school premises, including through the use of their own networks or other internet connections.

All staff (including operations staff), trustees and volunteers have particular legal and professional obligations, and it is imperative that all parties understand that online safety is part of safeguarding as well as part of the curriculum; it is everybody's responsibility to uphold the school's approaches, strategy and policy in this area.

Parents and carers will be informed about this Acceptable Use Policy and are expected to support its implementation.

This policy is part of a portfolio of policies addressing safeguarding and the conduct of students and staff.

Responsibilities

All users of IT equipment and services at Wilson's must agree to the following:

BEHAVIOUR:

- Anything I do, write, post or share using IT equipment will accord with the values of the school as set out in the relevant Code of Conduct / published standards (e.g. Teacher Standards).
- I will treat others with respect at all times, communicating using IT equipment as respectfully as I would face to face.
- I will always act to protect my reputation and that of the school, staff, students and others. I know that anything I do can be shared and may stay online forever - even disappearing or anonymous messages can be traced and saved. I know that data shared with many AI platforms is retained and used to train AI models.
- I will take action to change my behaviour if I am struggling to use IT responsibly and productively.
- I will not post, look at, up/download or share material that could be offensive, misleading, harmful or illegal. If I come across any, I will report it immediately.
- I will not access, share, or promote extremist or radicalising material. I understand that accessing or promoting such content may be a safeguarding concern under the Prevent Duty.

- I will not enter into any legally binding or contract agreement on behalf of or while representing the school, without authority to do so.
- I will not enter into or undertake any activity that could be classed as gaming or gambling, including crypto-gambling or loot boxes.
- I will not enter into or undertake any activity that may breach any copyright or licence agreement, including by sharing copyright material or personal data with large language models (AI).
- I will not utilise any means, mechanisms or tools to circumvent or otherwise undermine the school's internet controls or arrangements for network security.

<u>EQUIPMENT:</u>

- I will not damage, disable, or otherwise harm the operation of computer hardware. I will not eat or drink in a computer room or near school IT equipment in order to protect computers and other equipment from damage.
- I will report any problems with the equipment or systems to IT support as soon as practicable.
- I will protect any devices in my care from unapproved access or theft.
- I will always keep the OS and software up to date on mobile equipment that I use (e.g. laptops, tablet PCs, PDAs etc.) to minimise risk from viruses. I will 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.
- I will not remove labels from computers or other computer equipment or remove any equipment from the premises without signing it out in the IT loans book.

<u>ACCESS, SECURITY & SETTINGS:</u>

Use of the school's IT systems and internet connection is monitored and logged for security and safeguarding purposes, in line with UK GDPR Article 6(1)(e) (public task). Users should have no expectation of personal privacy when using school systems. The school is committed to meeting the DfE Filtering and Monitoring Standards. Monitoring is proportionate, risk-based, and overseen by the Designated Safeguarding Lead and Data Protection Officer.

- I understand that the school may be able to track my activity whenever I am on any school device or system, including school devices or systems when I am at home.
- When using any school IT equipment or service, I will use a strong, unique password, ensuring this has at least 12 characters, consisting of a mixture of upper and lower case alphabetical and numerical characters. I will not reuse passwords. I will enable multi-factor authentication (MFA) wherever this is available.
- I will keep login details secret, never disclosing my password or any security information to others, and change my password when instructed to do so. If I think someone knows my password, I will change it; if I think they have used it, I will inform a member of SLT immediately. I will not leave any information system unattended without first logging out or securing/locking access.

- I will 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 or network; hyperlinks must be treated with caution. If in doubt I will not open/click on the item and I will seek further advice.
- I will not try to bypass school security in any way or access any hacking files or tools.
- I will only edit or delete my own files and not (even try to) view, change or delete other people's files or user areas without their permission.
- I will not illegally download copyright-protected material (text, music, video, etc.).
- I will not attempt to install any software, including browser toolbars, or hardware in school without permission.
- I will ensure that school's IT systems are used lawfully and appropriately. I understand that the Computer Misuse Act 1990 makes the following criminal offences: to gain unauthorised access to computer material; to gain unauthorised access to computer material with intent to commit or facilitate commission of further offences or to modify computer material without authorisation.

Questions or concerns about data protection, information security, or lawful data processing should be directed to the school's Data Protection Officer (DPO). Contact details are available in the Data Protection Policy.

Additional responsibilities for students

- I will only use apps, sites and games I am old enough for. I know most social media and many AI platforms are restricted to those aged 13+ and games can have higher age ratings.
- When I am at school or using a school system or device, I will only use apps, sites or games which I know are appropriate for school use.
- I will always avoid taking risks online and anything which encourages hate or discrimination.
- I know just calling something banter doesn't make it okay - if it is upsetting it could become bullying and / or harassment.
- I will not use technology to bully, impersonate, harass, threaten, make fun of or upset anyone, at school or outside – or that could risk harming the reputation of the school. I will not be a bystander if I become aware of bullying online.
- I know people online might not be who they say they are, even if the picture and name are from someone I know, so I will always be very careful when someone wants to add me.
- I will always talk to a trusted adult (and take them with me the first time) before I meet someone face to face who I initially met online.
- I will only use my personal devices (mobiles, smartwatches etc) in school if I have been given permission and under supervision, and I will never take photos, videos or recordings, including when learning remotely, without the permission of a member of staff.
- I will check location and privacy settings the first time I install an app and regularly afterwards because many apps can show everyone where I am, where I live and go to school.
- I know that I do not have to keep a secret or do a dare or challenge just because someone (including a friend) tells me to. Even if I have promised to do something, if I then realise it is a bad idea, I don't have to do it.
- I can always say no online, end a chat or block someone; if I do, I know that I can talk to someone about it in school.
- I know it is illegal to look at pornography if you are under 18 so I will not attempt to do so and will report anyone who sends it to me or tries to trick me into it.
- I will respect my body and other people's. I will never share photos or videos to shame or embarrass, and I will never share images of myself, others (including children) not fully dressed. I understand that the possession of indecent photographs or pseudo photographs of children is a criminal offence. I understand that this includes AI-generated and/or deepfake images.
- I know that it is not my fault if I stumble across (or somebody sends me) something violent, sexual or otherwise worrying. But I will not share or forward it, and I will ask for advice/help without delay.
- I will not share my or others' personal information that can be used to identify me, my family or my friends on any online space, unless a trusted adult has given permission and reviewed the site.

- I will not attempt to contact any member of staff via social media; I know that all communication with members of staff must be via the school systems (i.e. email, SatchelOne, Arbor).
- I will always check sources before sharing, because I know any information I see online could be biased and misleading, and there are lots of spoof accounts. I am aware that many social media companies are reducing or entirely abdicating their responsibilities for checking news content for accuracy. News should come from a news site, not from a screenshot or a friend of a friend. If I share bad news, I will make sure there is evidence from a reliable source.

Additional responsibilities for members of staff and other adults:

- I acknowledge the place of this policy in ensuring the safeguarding of children in the school and I will raise any concerns relating to this policy or online safety promptly with the DSL.
- I understand that I am responsible for promoting online safety as part of a whole school approach in line with the PSHE curriculum, as well as safeguarding considerations including when supporting students remotely. I acknowledge that children often have unrestricted mobile internet even at school which can lead to unmonitored sexual harassment, bullying, control, indecent images (including deepfakes), pornography and other harmful content.
- I understand that in any periods of home learning, school closures or potential lockdowns, there is a greater risk for grooming and exploitation as children spend more time at home and on devices; I must play a role in supporting educational and safeguarding messages to help with this.
- I will ensure that any personal data is kept in accordance with the Data Protection legislation, including GDPR in line with the school/setting information security policies. I recognise that it is far preferable to use hyperlinks to folders on the school system rather than attaching documents (particularly those containing any personal data) to emails. Any such attachments **must** be password protected.
- I will not store school-related data on personal devices, storage or cloud platforms (other than the school Microsoft 365 account). USB keys, if allowed, will be encrypted, and I will only use safe and appropriately licensed software, respecting licensing, intellectual property and copyright rules at all times.
- I understand that I am a role model and will promote positive online safety and model safe, responsible and positive behaviours in my own use of technology, including social media and AI tools, e.g. by not sharing other's images or details without permission and by refraining from posting negative, threatening or violent comments about others, regardless of whether they are members of the school community or not.
- I will check, prior to use in a classroom setting, that any live internet materials (including any background banners, pop ups or 'suggested content') are not in breach of any of the provisions of this policy.
- I understand that any use of artificial intelligence (AI) tools for lesson planning, marking, communication, or administrative tasks must comply with data protection and safeguarding principles. Personal, student, or confidential data must never be entered into public AI systems. All AI outputs must be subject to human review.
- I will have regard to the **Prevent Duty Guidance (2023)** and report radicalisation concerns to the DSL.
- If my role requires me to confiscate or search an electronic device, I will act in line with DfE **Searching, Screening and Confiscation** guidance and the School Behaviour Policy.

Additional responsibilities relating to remote learning:

- I will uphold the same professional standards when interacting with students working remotely as I would if they were in school. I will never attempt to arrange any meeting, including tutoring session, without the full prior knowledge and approval of the school, and will never do so directly with a student. The same applies to any private/direct communication with a student.

- I will not attempt to use a personal system or personal login for remote teaching or set up any system on behalf of the school without SLT approval.
- I will not make secret recordings or screenshots of myself or students during live lessons.
- I will conduct any video lessons in a professional environment as if I am in school. This means I will be correctly dressed and not in a bedroom (or it will be impossible to tell that it is a bedroom if this is unavoidable). The camera view will not include any personal information or inappropriate objects and where it is possible to blur or change the background, I will do so.
- I will log and report any issues for live lessons immediately to the Designated Safeguarding Lead (if by a child) or Head (if by an adult) if anything inappropriate happens or anything which could be construed in this way. This is for my protection as well as that of students.

Use of Wi-Fi statement

All members of the school community should take measures to protect data and information systems from infection, unauthorised access, damage, loss, abuse and theft when using Wi-Fi.

All use of Wi-Fi must be in accordance with the school AUP and the law, including copyright and intellectual property rights. This includes the use of email, text, social media, social networking, gaming, web publications and any other devices or websites.

Wi-Fi agreement

- By using school Wi-Fi, I acknowledge that security errors and hacking are an inherent risk associated with any wireless network.
- I understand that my use of the school Wi-Fi will be monitored and may be recorded to ensure policy compliance in accordance with privacy and data protection legislation. If the school suspects that unauthorised and/or inappropriate use or unacceptable or inappropriate behaviour may be taking place, then the school may terminate or restrict usage. If the school suspects that the system may be being used for criminal purposes, the matter will be brought to the attention of the relevant law enforcement organisation.
- I will take all practical steps necessary to make sure that any equipment connected to the school Wi-Fi is secure, e.g. by ensuring up-to-date anti-virus software and systems updates. I understand that the school can accept no responsibility for any software downloaded and/or installed, email opened, or sites accessed via the school Wi-Fi connection to the internet. Any damage done to equipment for any reason including, but not limited to, viruses, identity theft, spyware, plug-ins or other internet-borne programs is the responsibility of the user.
- I will not attempt to bypass any of the school/setting security and filtering systems or download any unauthorised software or applications.

Use of email – guidance for staff

General expectations for use of email

- All members of staff are expected to check their school email account once per day on the days when they are working. All members of staff should be aware that some colleagues are part time. They are not expected to read or deal with email when they are not at work.
- All members of staff should be wary of the auto-complete function and ensure that all communications are sent to the intended recipient(s).
- It is almost always preferable to use hyperlinks rather than attachments. Attachments containing sensitive data must be password protected.
- Each user is responsible for the content of their Outlook account. If a member of staff is worried that they have received something inappropriate, they should contact a member of SLT and the IT Support team and delete the email promptly thereafter. Members of staff are responsible for managing the content of their mailboxes and following any instructions given about the retention of email.
- Members of staff must maintain a professional tone and content in all emails sent from a school email address. Great care must be taken when using AI tools to help compile emails, e.g. to ensure that personal information is not shared with AI models.
- 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.

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).

Use of email to communicate between staff and students.

- There is no expectation that subject teachers will use email to communicate with students.
- It is appropriate to email students at their school email address only to communicate about homework, missed work or other school related activity, such as participation in an extra-curricular activity.
- Use a courteous and reasonably formal and professional tone. Avoid banter, sarcasm or jokes or anything that may be considered over-familiar.
- Never discuss personal or confidential matters: theirs, yours or anyone else's.
- Do not use email to discuss behavioural matters or to set detentions.
- Never refer disparagingly to any person in an email to a student.

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.
- Head of Year to Cc Key Stage Director or a member of SLT.
- Members of SLT Cc to another member of SLT.
- Operations 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, Arbor (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 must be used.

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

Use of email to communicate between colleagues at Wilson's

- 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.
- 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.
- Avoid sending emails to colleagues at weekends wherever possible. If possible, use the 'delay delivery' option in Outlook.
- Remember that your emails are not private. While they are not continuously monitored, they can be accessed in controlled circumstances. Maintain a professional tone and content in all school emails.
- The use of online access to school email accounts is entirely voluntary. There is no expectation that staff should access their emails from home.
- If you need to forward an email to another colleague, consider whether you should seek permission to do so from the sender in advance.
- E-mails should not be sent advertising services or items for sale.

Use of email to communicate between staff and parents.

- At Wilson's, there is no expectation that subject teachers will use email to communicate with parents. 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).
- 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.
- 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.
- Emails to parents should be brief and to the point. Do not allow a disagreement with a parent to develop through email correspondence. If there is a significant disagreement, arrange a meeting to resolve it, engaging support from departmental or pastoral colleagues as appropriate.
- Never write in anger or frustration 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 or consider using an AI tool to moderate the tone of the email. 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.
- 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.
- 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 (e.g. CPOMS). 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.

Do not give parents your personal email address or any other personal contact details.

Acceptable Use Policy

Key Points for Students

Be Kind and Respectful

- Always treat others kindly online – the same as you would face-to-face.
- Never post, share, or say anything that could hurt, embarrass, or harm others.

Be Smart and Safe

- Keep your personal information private – never share passwords or addresses.
- Don't meet people in person who you only know online. Talk to a trusted adult if someone asks to.
- Report anything worrying or inappropriate straight away.

Be Legal and Honest

- Do not look for or share illegal or adult content.
- Never copy or download music, videos, or software without the appropriate permission.
- Don't use school systems for gaming, gambling, or anything illegal.

Be Responsible with Devices

- Look after school equipment and never eat or drink near computers.
- Only use your phone or smartwatch if you have permission and when under supervision.
- Keep your devices secure and updated.

Be Secure

- Use strong passwords.
- Never share your password – tell a teacher if you think someone knows it.
- Don't try to bypass school internet filters or install software.

Think Before You Post

- Anything you share online can last forever.
- Be careful with photos and videos – never share or forward nude or indecent images.
- Always check the truth of what you see online before sharing.

AI and Technology

- Only use AI tools approved by the school.
- Don't share personal data with AI or chatbots.
- Remember, YOU are responsible for anything you submit or create online.

If You’re Unsure – ASK!

- If something feels wrong or uncomfortable, talk to a teacher, your Head of Year, or the Designated Safeguarding Lead.