

WHITGIFT SCHOOL

STAFF AND VISITOR IT ACCEPTABLE USE POLICY

Colleagues responsible for this policy:

Rachel Attenborough (Senior Deputy)

Email: rra@whitgift.co.uk

Ally Tiltman (Director of Safeguarding/Designated Safeguarding Lead)

Email: a.tiltman@whitgift.co.uk

Most recent review: July 2026

Next review: July 2027

We are Whitgift: A diverse and grounded community where every person belongs - to a circle of friends, a team, a pursuit and a shared purpose. Here, pupils are known, nurtured and challenged. Through exceptional teaching, unrivalled opportunities and deep personal support of each boy, they become more: ready to step forward with confidence into their future.

Vision: Become more

Values: Belonging, Curiosity, Ambition, Respect, Courage

Whitgift School seeks to acknowledge the use of IT to enhance teaching, learning and administration within the school. It is necessary to outline the principles underpinning appropriate computer use, make expectations clear and ensure users are aware of how these devices should be used as members of the Whitgift School community.

This policy applies to:

- all Whitgift School staff who may have access to a school owned computer or the school network (either on school site or elsewhere).
- all visitors/guests of Whitgift School who may be connecting to the school network, either via school equipment or their own personal equipment

This document should be used in conjunction with the following related policies:

- Mobile, BYOD and Remote Access Policy
- AI Policy

- Online Safety Policy
- Safeguarding and Child Protection Policy
- Social Media and Communications Policy
- Staff Code of Conduct
- Staff Handbook

If you become aware of a breach of this policy or the Online Safety Policy, or you are concerned that a member of the school community is being harassed or harmed online, you should report it as follows:

- If your concern is about the conduct of a student, you should report it to the Director of Safeguarding/Designated Safeguarding Lead, or a Deputy DSL.
- If your concern is about the conduct of a member of staff, you should report it to the Director of Safeguarding or Headmaster.
- If your concern is about the conduct of the Headmaster, you should report it to the Chair of Governors.

Please note, Whitgift School reserves the right to update this policy at any time.

General Computer Use

- Priority for computer usage should always be given to the core functions of the school.
- Use of IT equipment (such as computers and printers), email and the internet within the school should be primarily to enhance teaching and learning or for administrative use.
- Users are not to engage in hacking or use hacking software/paraphernalia on a computer or network account.
- Staff are not to engage in physical interference with another user's computer or school owned computer.
- No attempt should be made to circumvent the content filters or other security measures installed on the school's IT systems.
- By using personal devices for work purposes, device owners shall be responsible for keeping the device and the school's information protected. Device owners shall:
 - Set passwords, PINs (at least 6 characters) or biometric controls used to unlock devices in line with the school's operating system's password expectations.
 - Immediately report any security incidents, events or weaknesses to Whitgift School's IT Support department.
 - Keep devices up to date with latest security updates.

Refer to the Mobile, BYOD and Remote Access policy for more details.

User and Guest Accounts

- User accounts are the responsibility of the user.
- Passwords must be kept secure and changed once a year, as a minimum, and be of sufficient complexity to not be considered easily guessable.
- Users must not allow anyone else to use their school account nor should they use a colleague's school account.
- Users must not share their usernames and passwords with anyone else.
- Users must log off or **lock their account when away from their machine**. Accounts are not to be left logged in and unattended.
- When working from home / off site, there must be careful consideration around connecting to public Wi-Fi and screen visibility in public spaces.

- If working abroad, staff are expected to inform IT before they travel.
Please refer to Mobile, BYOD and Remote Access Policy for more details.

Internet Usage

- Internet connectivity within the school is provided to enhance teaching and learning or for administrative use.
- It is understood that users may occasionally need to use the internet for personal reasons; this should not be at the expense of work nor to undertake activities that the school would consider unethical or illegal.
- Staff must not search for, or browse through, any sites that contain offensive, obscene, violent, dangerous or inflammatory material, or gambling, unless this is with the express permission of a member of the Senior Leadership Team for the purposes of testing school filtering and monitoring systems, or for the purposes of teaching an aspect of the curriculum.
- Staff are discouraged from using their school issued devices to access their own social media sites. This includes, but is not limited to, Instagram, Facebook, TikTok, Snapchat, WhatsApp and X.
- Staff must not engage in any activity that may compromise their responsibilities or integrity. This includes creating content that is inappropriate.
- Staff should ensure that their online communications, including shared content, is respectful of others.
- Staff should respect the privacy of others. They should not share photos, videos, contact details, or other information about members of the school community, even if the content is not shared publicly, without their express permission.
- Staff should not name or make it obvious that they are referencing a particular colleague on social media unless they have express permission from the colleague in question to do so.

Use of Personal Devices

- Staff must be aware that this Acceptable Use Policy applies to their use of personal equipment on the premises or in situations related to their employment by the school.
- Staff must be aware when using a personal device and accessing the Whitgift network (WiFi) that filtering still applies and certain activities will be blocked and recorded.
- Staff must be aware that all rules set out in this Acceptable Use Policy must be adhered to when using any school equipment or systems. This includes the use of school equipment and services when away from Whitgift School, as well as using a personal device to access Whitgift services.
- Staff must ensure that all personal devices used to access school systems have at least the operating system's default anti-malware software enabled and preferably its designated anti-malware software installed.

Hardware and Software

- All users are responsible for the care and safe-keeping of any IT equipment under their supervision – this includes but is not limited to: laptops, portable electronic devices, tablets, school mobile phones, desktop computers in classrooms, offices and common areas.
- Users will not download and install software packages without the authorisation of the Head of IT.
- If a staff member would like to purchase and/or install new software (including AI platforms), the user must complete a [Whitgift Software Proposal Form – Fill in form](#) or [Whitgift AI Tool Proposal Form – Fill in form](#) . IT Steering will then review the submission for approval. If approved, IT will then install.
- Any IT hardware or software purchased for school purposes must be actioned through the

IT Support Department to ensure suitable compliance with existing systems and future proofing.

- Old and broken equipment to be disposed of must be actioned through the IT Support Department as disposal of electrical equipment is subject to UK government regulations.

Data

- Data must be kept in accordance with the GDPR and the John Whitgift Foundation's Data Protection Policy.
- Data within AI should only be used in conjunction with Whitgift's AI Policy.
- Staff must not disclose any information to a third party that could be considered personal data, unless authorised to do so.
- School systems and devices should not be used to store personal data.
- Unlicensed material should not be brought into school and copied on to the school systems.
- Staff must ensure that when they take and/or publish images of others, they do so with the other party's permission.
- Data should not be copied from the school systems onto unsecured storage devices.
- Data on current, future, and past students, parents, and staff should only be used for the express purposes of undertaking school activities.

Electronic Communication

Staff should be aware of the professional risks involved in communicating with students via non-school managed systems such as instant messaging, mobile phones, or text messaging, though the School recognises that there are situations (for example, on School trips or in emergencies) where there is no alternative. Any concerns about this area should be discussed with the Director of Safeguarding/Designated Safeguarding Lead, the Senior Deputy or with another senior colleague.

- Emails sent using the school email system should be used only in a professional capacity.
- Sometimes, email communication can be misinterpreted – especially in its tone – and a conversation may be better, particularly when dealing with a sensitive matter. Staff should consider carefully their use of electronic communication before sending.
- Staff should not open or forward any email or attachment from an unrecognised source or that they suspect may contain inappropriate material or viruses.
- Staff should not respond to emails that request personal details, unless you are confident the source is genuine. In general, companies will not request personal data via email.
- If they are concerned about any email that they have received, staff should contact the IT Support Department.
- Contacting students and parents electronically should only be undertaken using a school-managed system, such as school email, Microsoft Teams, or Firefly to provide an audit trail. This includes those who are yet to join the school, those who are currently at the school and those who have left the school.
- Any data that is sent to external addresses is potentially subject to the GDPR and consideration should be given to whether the communication will need to be encrypted. Please speak to the Director of Estates and Facilities if you are unsure whether the communication needs to be encrypted.

Social Networking and Websites

Some useful guidance is provided below, but staff should also ensure that they have read and adhere to the Social Media and Communication Policy.

- Staff should think very carefully before participating in social networking sites and should check privacy settings very carefully as well as the authenticity of any contacts, shared material, and links.
- Any communication made or information placed on the internet must not bring the School into disrepute, refer to students, parents or other members of staff, or undermine the professional standards of a member of staff.
- If a member of staff wants to post information on the internet relating to their role at Whitgift (for example, an education blog), permission should be sought from the Headmaster in advance.
- Staff should not communicate with current students and parents on social media or non-school approved communication platforms.
- Staff should not accept connections on LinkedIn until students have been off Whitgift school roll for a minimum of 3 years. Even after this time, advice is to accept requests with caution and any correspondence should still be professional.
- Whitgift understands that some staff may have existing connections with previous Whitgift students when they join our staff. This connection should be reported to the Director of Safeguarding/DSL.
- Staff should be aware that when accepting contact requests from former students or former parents, these individuals may still have contacts in the Whitgift School student community.
- All staff communication with parents for school matters should be through the platforms listed below:
the School's email system (Outlook)
Microsoft Teams
ISams
Involve

General Usage

- Staff and visitors will not browse, create, store, or copy content of a nature which might be considered inappropriate for the workplace, using a school device or on a school network.

Monitoring

As an employer which takes safeguarding seriously, all laptops owned by Whitgift School are monitored. Monitoring aids Whitgift School in fulfilling its legal duty of care around online safety and safeguarding. The school also employs a platform which monitors attempts to access inappropriate sites.

The Director of Safeguarding oversees the monitoring of both staff and student school devices. If a staff member enters words or phrases which appear in the school's catalogue of triggers, the screen will be captured and seen by the Director of Safeguarding. Staff must be aware of this when using their school devices and take this into consideration when using the laptop for anything other than school related tasks.

The Director of Safeguarding is responsible for flagging all staff misuse of IT to the Headmaster. The IT Support Department has access to Senso/Securus but does not undertake any monitoring of staff. All reviewing of staff activity is logged and logs are not erasable.

Any form of violation of this policy may call for disciplinary measures under Whitgift School's staff disciplinary policies.