

IAT Information and Communication Technology (IT) Policy

Issued: October 2026



Insignis
Academy Trust

Collaborate to Succeed

IAT Information and Communication Technology (IT) Policy

Issued: October 2026



Approved by	IAT Board of Trustees
Approval date	October 2026
Recommended review date	November 2027

This policy pertains to Insignis Academy Trust (IAT) and all of its schools, including any school which joins the Trust during the period of this policy.

IAT Information and Communication Technology (IT) Policy

Issued: October 2026



Contents

1	Introduction, Aims, Purpose, and Scope	5
2	Legislation and Guidance	5
3	Definitions	6
4	Roles and Responsibilities	6
4.1	The Trustees	6
4.2	COO and Head of Operations	7
4.3	The Headteacher/Head of School	7
4.4	The Designated Safeguarding Lead (DSL)	7
4.5	The IT Managed Service Provider (MSP) Lead	7
4.6	All Staff and Volunteers	7
5	Protection of the IAT Network and Use of Computer Equipment.....	7
6	Unacceptable Use	8
6.1	Illegal and Harmful Content and Conduct	8
6.2	System Misuse and Security Breaches	9
7	Filtering and Monitoring the IAT Network and Use of IT Facilities	9
7.1	System Standards	9
7.2	Annual Audit and Board Review.....	9
7.3	Monitoring Scope	10
8	Data Security and Cyber Protection.....	10
8.1	Passwords and Authentication.....	10
8.2	Software, Encryption, and System Security	11
8.3	Data Access and Remote Work.....	11
8.4	Protection from Cyber Attacks	11
9	Staff (Including Trustees, Governors, Volunteers, and Contractors) Use of IT	12
9.1	Access to IAT IT Facilities and Materials	12
9.2	Email and Electronic Communications.....	12
9.3	Use of IAT Phones	13
9.4	Personal Use of IT Facilities	13
9.5	Personal Mobile Phone Use (Staff)	13
10	Social Media and Professional Boundaries	14
10.1	Official IAT/school Accounts.....	14
10.2	Staff Personal Accounts	14
11	Students and Mobile Phones	15
11.1	Access to IT Facilities	15
11.2	Mobile Phone Use (Students)	15
11.3	Online Safety Curriculum and Cyber-bullying	15
11.4	Search, Screening, and Confiscation	15

IAT Information and Communication Technology (IT) Policy

Issued: October 2026



12	Parents/Carers and Visitors	15
12.1	Access to IT Facilities and WiFi	15
12.2	Online Communication Expectations	16
13	Virtual Meetings (Governors/Trustees)	16
14	Sanctions	17
14.1	Staff	17
14.2	Students	17
15	Related Policies	17
16	Review and Version Control	17
Appendix 1: Acceptable Use Agreement (Staff, Trustees, Governors, Volunteers and Visitors)		18
Appendix 2: Acceptable Use Agreement (Secondary School students)		22
Appendix 3: Acceptable Use of the Internet – Agreement for Parents and Carers		25
Appendix 4: Glossary of Cyber Security Terminology		26

1 Introduction, Aims, Purpose, and Scope

Information and communications technology (IT) is an integral part of the way Insignis Academy Trust (IAT) and its schools operate. It is a critical resource for students, staff, Trustees, Governors, volunteers, contractors and visitors. The safe and efficient management of IT resources and facilities is necessary to reduce risks relating to data protection, online safety, and safeguarding.

This policy covers all users of IAT's IT Facilities, including Trustees, Governors, staff, students, volunteers, contractors, and visitors.

This policy aims to set out the rules and guidelines on the use of IAT IT networks and systems, establish clear expectations for online engagement within the IAT community, support policies on data protection, online safety, and safeguarding, prevent disruption from misuse, and support the teaching of safe and effective IT use.

Any concerns or clarifications regarding this policy should be discussed with the IAT Head of Operations in the first instance.

2 Legislation and Guidance

This policy refers to, and complies with, the following legislation and guidance:

- Data Protection Act 2018.
- The UK General Data Protection Regulation (UK GDPR).
- Computer Misuse Act 1990.
- Data (Use and Access) Act 2025.
- Worker Protection (Amendment of Equality Act 2010) Act 2023.
- Department for Education (DfE) Guidance: Mobile phones in schools.
- Human Rights Act 1998.
- The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000.
- Education Act 2011.
- Freedom of Information Act 2000.
- Education and Inspections Act 2006.
- Keeping Children Safe in Education 2026.
- Searching, screening and confiscation: advice for schools 2022.
- National Cyber Security Centre (NCSC): Cyber Security for Schools.
- UK Council for Internet Safety (et al.) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people.



3 Definitions

This policy refers to IAT throughout, and this should be read to include all or any of its schools.

IT Facilities	All facilities, systems, and services, including but not limited to: network infrastructure including wi-fi, desktop computers, laptops, Chromebook, tablets, phones, music players/hardware, interactive whiteboards, software, licences, websites, web applications or services, and any device or service provided as part of IAT's service.
Users	Anyone authorised by IAT to use the IT Facilities, including Trustees, Governors, staff, students, volunteers, contractors, and visitors.
Personal Use	Any use or activity not directly related to the user's employment, study, or purpose agreed by an authorised user.
Authorised Personnel	Subcontractors or employees authorised by IAT to perform systems administration and/or monitoring of the IT Facilities. Specifically named personnel include the COO, Head of Operations, and IT MSP Lead.
Materials	Files and data created using IAT's IT Facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs.
Mobile Phones	Refers to mobile phones and similar devices, including smartphones, and all devices with communications and smart technology that IAT chooses to include in their policy, such as smartwatches.
Social Media	Includes all technologies that allow individuals to communicate and share information (including photos and video), such as group messaging services like WhatsApp.

4 Roles and Responsibilities

4.1 The Trustees

The IAT Trustees have overall responsibility for monitoring this policy and holding the COO, Head of Operations and Headteacher/Head of School to account for its implementation. The Trustees are responsible for making sure that:

- IAT complies with DfE guidance on digital standards.
- Staff are aware of those systems and trained in their related roles and responsibilities.



4.2 COO and Head of Operations

The Chief Operating Officer (COO) is responsible for:

- Ensuring that the policy is current and effective.
- Ensuring that the staff are aware of their responsibilities arising from this policy.

The Head of Operations will manage the day-to-day activities that arise from these responsibilities and ensure they are implemented by the MSP.

4.3 The Headteacher/Head of School

The Headteacher/Head of School is responsible for ensuring that all IAT school staff understand this policy and that it is being implemented consistently throughout IAT.

4.4 The Designated Safeguarding Lead (DSL)

The DSL takes lead responsibility for online safety in IAT. This includes taking the lead on understanding the filtering and monitoring systems and processes, working with the Head of Operations and IT MSP Lead to ensure appropriate systems are in place, responding to safeguarding concerns identified by filtering and monitoring, and managing and logging all online safety issues and incidents and ensuring staff are trained to recognise online risks.

4.5 The IT Managed Service Provider (MSP) Lead

The IT MSP Lead manages access to IAT's IT Facilities. The IT MSP Lead is responsible for:

- Putting in place appropriate filtering and monitoring systems on IAT devices and networks.
- Ensuring IAT's IT systems are secure and protected against all forms of cybersecurity threat including viruses and malware.
- Blocking access to potentially dangerous sites.

4.6 All Staff and Volunteers

All staff (including Trustees, Governors, contractors and agency staff) and volunteers are responsible for maintaining an understanding of and consistently implementing this policy, agreeing and adhering to the terms on acceptable use (Appendix 1), being aware of how to report incidents of filtering/monitoring systems failing, and responding appropriately to all reports and concerns about sexual violence and/or harassment.

5 Protection of the IAT Network and Use of Computer Equipment

To prevent viruses and malware from being introduced into the IAT IT Facilities, the following mandatory rules must be strictly adhered to:

Software Management and Use



- All software must be authorised and checked by the IT MSP team before installation or use.
- The use of unauthorised software is strictly prohibited.
- Software use is limited exclusively to official IAT applications, teaching, and learning purposes.
- If new software will access or use any personal data, a Data Protection Impact Assessment (DPIA) must be completed and approved beforehand.

Hardware and Procurement

- No hardware or software may be purchased without prior authorisation from Authorised Personnel.

Compliance and Security

- Unauthorised copying and/or removal of IT Facilities will lead to disciplinary action.
- Extreme caution must be exercised when accessing external emails to prevent the introduction of malware via phishing links or the accidental sharing of confidential information.

6 Unacceptable Use

Users of IAT's IT Facilities must adhere strictly to this policy. Failure to comply may result in action under the IAT Behaviour Policy or the IAT Conduct and Discipline Policy. Users should be aware that some instances of unacceptable use may also constitute a criminal offence.

Note for Students: The following items remain applicable to usage outside of school hours when using school managed devices via a school account. Breaches of these rules outside of school may still lead to sanctions under the IAT Behaviour Policy.

6.1 Illegal and Harmful Content and Conduct

- a) Using the IT Facilities to breach intellectual property rights or copyright.
- b) Using the IT Facilities to bully or harass someone else, or to promote unlawful discrimination.
- c) Breaching IAT policies or procedures.
- d) Any illegal conduct, or statements which are deemed to be advocating illegal activity.
- e) Online gambling, inappropriate advertising, phishing and/or financial scams.
- f) Accessing, creating, storing, linking to, or sending material that is pornographic, offensive, obscene or otherwise inappropriate or harmful.
- g) Consensual and non-consensual sharing of nude and semi-nude images and/or videos and/or livestreams.
- h) Activity which defames or disparages IAT/the school, or risks bringing IAT/the school into disrepute.
- i) Sharing confidential information about IAT, its students, or other members of the



IAT community.

- j) Using inappropriate or offensive language.
- k) Engaging in content or conduct that is radicalised, extremist, racist, anti-Semitic or discriminatory in any other way.

6.2 System Misuse and Security Breaches

- a) Connecting any device to IAT's IT network without approval from Authorised Personnel.
- b) Setting up any software, applications, or web services on IAT's network without approval by Authorised Personnel.
- c) Creating or using any programme, tool, or item of software designed to interfere with the functioning of IAT's IT Facilities, accounts, or data.
- d) Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from Authorised Personnel.
- e) Allowing, encouraging, or enabling others to gain, or attempt to gain, unauthorised access to IAT's IT Facilities.
- f) Causing intentional damage to IAT's IT Facilities.
- g) Removing, deleting, or disposing of IAT's IT equipment, systems, programmes, or information without permission from Authorised Personnel.
- h) Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not permitted by Authorised Personnel to have access, or without authorisation.
- i) Using websites or mechanisms to bypass IAT's filtering or monitoring mechanisms.
- j) Promoting a private business, unless that business is directly related to IAT.

7 Filtering and Monitoring the IAT Network and Use of IT Facilities

To safeguard and promote the welfare of children and provide a safe environment to learn, IAT reserves the right to filter and monitor the use of its IT Facilities and network. Users consent to this monitoring.

7.1 System Standards

IAT will maintain filtering systems that block access to illegal and harmful content, including Child Abuse Image Content (CAIC). These systems will be provided by a member of the Internet Watch Foundation (IWF).

7.2 Annual Audit and Board Review

A formal technical audit of filtering and monitoring systems will be conducted annually. The results will be shared with the DSLs and the Board of Trustees to ensure IAT remains



compliant with the latest DfE standards.

7.3 Monitoring Scope

Monitoring includes, but is not limited to, the filtering and monitoring of:

- Internet sites visited.
- Bandwidth usage.
- Email accounts.
- Telephone calls.
- User activity/access logs.
- Any other electronic communications.

Only authorised IT personnel may filter, inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law.

IAT monitors use of its network and any connected devices in order to:

- Obtain information related to IAT business.
- Investigate compliance with IAT/school policies, procedures and standards.
- Ensure effective IAT and IT operations.
- Conduct training or quality control exercises.
- Prevent or detect crime.
- Comply with a subject access request, Freedom of Information Act request, or any other legal obligation.

IAT's Head of Operations and Designated Safeguarding Leads (DSLs) will take lead responsibility for understanding the filtering and monitoring systems and processes in place. Where appropriate, staff may raise concerns about monitored activity with their DSL and/or the Head of Operations.

8 Data Security and Cyber Protection

IAT is committed to maintaining the appropriate level of security to protect its systems, staff, and students. To achieve this, IAT aims to comply with the cyber security standards recommended by the DfE's guidance on digital and technology standards for schools and colleges. These measures include implementing firewalls, security features, user authentication, multi-factor authentication, and anti-malware software.

8.1 Passwords and Authentication

- All users of IAT's IT Facilities must set strong passwords for their accounts and ensure they remain secure. Users are individually responsible for the security of their passwords and accounts.
- The disclosure of account or password information may result in disciplinary action for staff and students, and access rights being revoked for parents, visitors, or volunteers.



- Staff should use Google Password Manager or other IAT-approved password management solution to help them store their passwords securely.
- Staff[GB1][AB2] must enable multi-factor authentication (MFA) on IAT IT accounts and any other IAT-managed system (where available).

8.2 Software, Encryption, and System Security

- **System and Device Management:** the IT Managed Service Provider (MSP) Lead is responsible for ensuring all IAT IT devices are maintained with current software, patches, security updates, and anti-virus protection.
- **User Compliance:** users must not attempt to bypass or circumvent any of the administrative, physical, or technical safeguards implemented and maintained by IAT.
- **Data Protection:** all personal data must be processed and stored in compliance with data protection regulations and the IAT Data Protection Policy.
- **Technical Safeguards:**
 - IAT will ensure an appropriate level of encryption is used on its devices and systems.
 - a firewall will be in place and operational at all times.

8.3 Data Access and Remote Work

- All users of IAT's IT Facilities will have clearly defined access rights to IAT systems, files and devices. These access rights are managed by IT MSP.
- Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert IT MSP immediately.
- Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and shut down completely at the end of each working day.
- **Remote Access:** IAT allows staff to access IT Facilities and Materials remotely. Staff must abide by the same rules as apply when accessing the facilities on-site and must be vigilant to protect personal data and against the risk of Cyber-attacks.
- **Personal Devices:** staff should ensure IAT data is not stored on personal devices. Staff[GB3][AB4] are also responsible for ensuring any personal device which is used to access IAT systems is protected with the appropriate levels of security and encryption.

8.4 Protection from Cyber Attacks

To protect against cyber attacks, IAT will implement a multi-layered, proportionate, and regularly reviewed set of controls:

Staff Training & Awareness

- Provide mandatory annual cyber security training for all staff[GB5][AB6], including as part of induction.



- Ensure all **staff** **[GB7]** **[AB8]** are aware of the procedures for reporting and responding to cyber security incidents.

Security Management & Review

- Delegate specific responsibility for maintaining the security of the management information system (MIS).
- Require IT staff to conduct regular access reviews.
- Check and ensure the security of the supply chain.
- The IT MSP Lead and Head of Operations will undertake an annual review of the effectiveness of filtering and monitoring systems and report their findings to the IAT Board.
- A formal technical audit, such as 360 degree safe, will be completed annually, with results shared with the DSL group and Trustees to ensure compliance with DfE standards.
- Business Continuity Planning.

Incident Response & Data Protection

- IAT will not engage with or pay ransom requests related to ransomware attacks.
- Develop, review, and test an incident response plan with the IT department. This plan will be reviewed and tested **every 6 months** and after any significant event, using the NCSC's 'Exercise in a Box' tool.
- Back up critical data in line with NCSC best practice guidance and store these backups securely (e.g., on cloud-based backup systems or external hard drives not connected to the network).

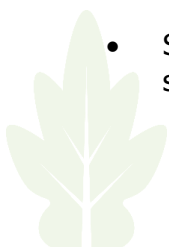
9 Staff (Including Trustees, Governors, Volunteers, and Contractors) Use of IT

9.1 Access to IAT IT Facilities and Materials

Access to IAT's IT Facilities (except IAT phones) and Materials for IAT staff is managed by IT MSP. Staff are provided with unique login/account information and passwords that they must use. This password must never be shared with any student or other member of staff. When leaving IAT, staff must notify the Authorised Personnel of all access passwords.

9.2 Email and Electronic Communications

- The IAT provided email account should be used for work purposes only, and all work-related business should be conducted using this account.
- Staff must not share their **personal email addresses** **[GB9]** **[AB10]** with parents/carers and students and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims (e.g., discrimination, harassment, breach of



confidentiality). Emails are potentially retrievable and may be subject to disclosure in legal proceedings.

- Attachments containing sensitive or confidential information should be encrypted.
- If staff receive an email in error, the sender should be informed and the email deleted. If the email contains sensitive information, the user must not make use of or disclose that information.
- If staff send an email in error that contains personal information, they must inform the Data Protection Lead (DPL) immediately.

9.3 Use of IAT Phones

IAT uses 3CX for its phone system.

- Staff must use IAT provided phones, or 3CX through their staff computer, to conduct all work-related business.
- Staff must not give their personal phone number(s) to parents/carers or students.
- Where required, staff will be provided with a mobile phone and must abide by the rules for IT unacceptable use set out in Section 6.

9.4 Personal Use of IT Facilities

Staff are permitted occasionally to use IAT IT Facilities for personal use, provided that such use:

- Does not take place during allocated working time (or contact time/teaching hours/non-break time).
- Does not constitute unacceptable use, as defined in Section 6.
- Takes place when no students are present.
- Does not interfere with their jobs or prevent others from using the facilities.

Staff may not use IAT IT Facilities to store personal, non-work-related information or materials (such as music, videos or photos). Staff should be aware that personal use may put communications within the scope of IAT's monitoring activities.

9.5 Personal Mobile Phone Use (Staff)

Staff are permitted to use their personal devices in line with the IAT Code of Conduct.

- Staff are not permitted to use their personal mobile phone for personal reasons in front of students throughout the school day. Use must be restricted to non-contact time and to areas where students are not present.
- Staff must not use personal mobile phones to process personal data or any other confidential IAT/school information.
- Staff must not use personal mobile phones to take photographs or recordings of students, their work, or anything else that could identify a student. IAT equipment must be used if necessary.



10 Social Media and Professional Boundaries

10.1 Official IAT/school Accounts

Official social media accounts (e.g., Facebook, Instagram, LinkedIn) exist for IAT and each school. Management of these accounts is the responsibility of authorised staff members.

Authorised managers/posters will not post:

- Names and photos of individuals without consent.
- Harmful or abusive comments.
- Messages to specific people.
- Political statements.
- Advertisements to businesses unless directly related to IAT.
- Links to staff members' personal accounts.

Authorised staff will delete as soon as reasonably possible: abusive, racist, sexist, homophobic or inflammatory comments, spam, personal information, and posts that advertise commercial activity or ask for donations. If users are repeatedly abusive or post inappropriate content they will be blocked.

10.2 Staff Personal Accounts

Staff must consider the safety of students and the risks to IAT when using social media channels, including when doing so in a personal capacity. Staff must follow IAT's guidelines on use of social media (see IAT Code of Conduct).

When using personal social media, staff must not:

- Use personal accounts to conduct IAT business.
- Accept 'friend requests' from, or communicate with, present students. Past students can be 'friended' after clearing this with CEO/Executive Headteacher/Headteacher/Head of School.
- Complain about IAT or any of its schools, individual students, colleagues, or parents/carers.
- Post images of students.
- Link their social media profile to their work email account.
- Associate themselves with IAT or any of its schools on their profile (e.g., by setting it as their workplace).

Any communication received from current students (unless family members) on any personal social media accounts must be reported to the DSL or senior leadership team immediately.



11 Students and Mobile Phones

11.1 Access to IT Facilities

Students sign an acceptable use agreement on joining their school. Access provisions include managed Chromebook, BYOD (Bring Your Own Device) policies, sixth form access, IT suites, and other devices[GB13][AB14]. Provision includes unique login passwords.

11.2 Mobile Phone Use (Students)

The use of mobile phones by students in school is covered by the IAT Behaviour Policy. In line with DfE guidance, all IAT schools are mobile phone-free environments by default for the duration of the school day.

IAT accepts no responsibility for mobile phones that are lost, damaged, or stolen on school premises, transport, or during school visits.

11.3 Online Safety Curriculum and Cyber-bullying

Students will be taught about online safety as part of the curriculum. This includes learning how to use technology safely, identify where to seek help, recognise acceptable behaviour, understand how principles apply to online relationships, and how to protect online privacy and identity. The school will actively discuss cyber-bullying and treat any use of AI to bully students very seriously.

11.4 Search, Screening, and Confiscation

The Headteacher/Head of School, and any authorised member of staff, can search and confiscate students' electronic devices if they have reasonable grounds for suspecting the device poses a risk to staff or students, is a banned item, or is evidence in relation to an offence.

- **Examination and Erasing:** authorised[GB15][AB16] staff may examine, and in exceptional circumstances erase, data or files on a confiscated device where they believe there is a 'good reason' to do so (e.g., to prevent harm or disrupt teaching). In this context authorised staff are the CEO, COO, Head of Operations and staff given delegated authority on a case-by-case bases with permissions granted accordingly.
- **Indecent Images:** if a staff member suspects a device may contain an indecent image of a child, they must not view the image, but should confiscate the device, and report the incident to the DSL immediately.
- **Legal Evidence:** if material may constitute evidence relating to a suspected offence, it will not be deleted, and the device will be handed to the police.

12 Parents/Carers and Visitors

12.1 Access to IT Facilities and WiFi

Parents/carers and visitors do not have access to IT Facilities as a matter of course. All IAT WiFi connections are secure.



Parents/carers, volunteers, and visitors may be granted access, or permitted to use IT Facilities, at the Executive team's/Headteacher's/Head of School's discretion if:

- They are working for, or with, the school/IAT in an official capacity (e.g., as a volunteer or a member of the PTA).
- Visitors need to access the school's WiFi in order to fulfil the purpose of their visit (e.g., to access materials for a presentation).

Where access is granted, the user must abide by this policy as it applies to staff.

12.2 Online Communication Expectations

Parents/carers are asked to sign the agreement in Appendix 3. When communicating with or about IAT and/or the school online, parents/carers should:

- Be respectful towards members of staff, IAT and the school, and other parents/carers.
- Direct any complaints or concerns through IAT's official channels.
- Not use private groups, IAT's or the school's social media page, or personal social media to complain about or criticise members of staff.
- Not use private groups or social media to try to resolve a behaviour issue involving other students.

IAT takes a firm stance against the harassment of staff by third parties, including parents and visitors. Abusive or derogatory online communication directed at staff via social media, private groups, or email will be treated as third-party harassment. In such cases, IAT will take active steps to protect staff, which may include warning the individual, banning them from premises, or terminating any existing contracts.

Parents/carers must also adhere to restrictions on mobile phone use on an IAT site, meaning they should not take pictures or recordings of students (unless at a public event or of their own child) or use phones in lessons or when working with students[GB17][AB18].

13 Virtual Meetings (Governors/Trustees)

The Trust Board/Local Governing Body can approve alternative arrangements for governors/trustees to participate or vote at meetings, including by telephone or video conference.

- **Attendance Protocol:** attendees should remain on mute unless speaking, say their name before speaking, and attend with the webcam/video switched on where possible. Attendees must prevent unauthorised individuals overhearing conversations and be mindful of their surroundings to ensure privacy.
- **Quorum:** all governors/trustees attending virtually count towards the quorum.
- **Voting:** governors/trustees may vote on any agenda item for which they have been fully present. Secret ballots will be allowed where possible, by sharing the vote privately with the chair/clerk.
- **Recording:** only the clerk has permission to record the meeting, and only if all attendees agree at the start. The recording will be handled in line with UK GDPR and deleted once no longer needed.



14 Sanctions

14.1 Staff[GB19]

Staff who engage in unacceptable activities may face disciplinary action in line with IAT's policies on staff discipline/conduct. Unauthorised or inappropriate use of the internet or e-communications may result in disciplinary action, including summary dismissal. Information acquired through monitoring may be used as evidence.

Reporting Digital Harassment

Staff who feel they are being bullied or harassed by a colleague or third party through digital means should refer to the IAT Anti-Bullying and Anti-Harassment Policy for formal and informal reporting procedures.

14.2 Students

Where a student misuses IAT's IT systems or internet, procedures set out in the IAT Behaviour Policy and acceptable use agreement will be followed, with action taken being proportionate to the severity of the incident. Incidents involving illegal activity will be considered for reporting to the police.[AB20]

15 Related Policies

This policy should be read alongside the IAT or school's policies on:

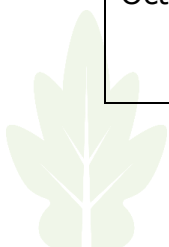
- Safeguarding and child protection (school level)
- IAT Behaviour Policy
- IAT Conduct and Discipline Policy
- IAT Code of Conduct
- IAT Data Protection (GDPR) Policy
- IAT Privacy notices
- IAT Complaints Policy
- IAT Photographic Images Policy

Please also refer to IAT Digital Strategy and IAT Use of Generative AI Protocol.

16 Review and Version Control

This policy will be reviewed annually to ensure continued alignment with the IAT Anti-Bullying and Anti-Harassment Policy and changing DfE statutory guidance.

Date	Comments
October 2026	New formal policy, based on templates available through Governor Hub/The Key, combined into one policy with the assistance of the NotebookLM AI tool.



Appendix 1: Acceptable Use Agreement (Staff, Trustees, Governors,[GB21][AB22] Volunteers and Visitors)[AB23]

(This form will be shared through iTrent for agreement by each staff member, Trustees and Governors; volunteers and visitors will be required to sign a copy of this form if they will be given access to the school's or IAT's IT Facilities.)

The school's IT systems are owned by Insignis Academy Trust (IAT) and may be used by staff to enhance their professional activities including teaching, research, administration and management. IAT reserves the right to examine, review and delete any files that may be held on its network and computer systems and monitor the visiting of any internet websites or mobile device apps.

Staff or third parties requesting access to the network or/and IT systems need to sign a copy of this Acceptable Use Agreement and return it to the school. Only then will computer and internet access be granted.

IAT reserves the right to revoke the use of its network, IT systems and equipment at any time.

1 For my professional and personal safety:

- 1.1 To safeguard students and staff I understand that IAT will monitor my use of the network and computer systems, email and other digital communications. Any illegal or undesirable activity will be reported to all appropriate agencies.
- 1.2 I understand that the rules set out in this agreement will also apply to all IT systems used by IAT (e.g. laptops, tablets, emails, Remote Access, VLE, Arbor).
- 1.3 I understand that IAT IT systems are primarily intended for educational use and that its use for personal or recreational use is in accordance with the policies and rules set by the school in this Acceptable Use Agreement.
- 1.4 I will not disclose my username or password to any third party, nor will I use any other person's username and/or password. I understand that I should not write down or store a password where it is possible that someone may access it and I should change my password on a regular basis.
- 1.5 I will immediately report any illegal, inappropriate or harmful material or incident, I become aware of, to the appropriate person.
- 1.6 Any activity that threatens the integrity of IAT and its IT systems, or attacks or corrupts other systems is forbidden and will be reported to the appropriate agencies.
- 1.7 Use of the internet for financial gain, gambling purposes, personal online purchases or advertising is forbidden.
- 1.8 I understand that any app/programme installed onto a school device is the property of IAT.
- 1.9 Social network sites should not be used in any IAT school. Staff must not communicate with students or parents on social network sites such as Facebook and Instagram.[GB24][AB25]

2 I will be professional in my communications and actions when using IAT IT systems

- 2.1 I will not access, download, remove or otherwise alter any other user's file or



apps, without the express permission of the IAT IT MSP Lead.

- 2.2 Use of the network and IT systems to access inappropriate materials such as pornographic, racist or offensive material is forbidden and will be reported to all appropriate agencies.
- 2.3 I am responsible for all e-mail sent and for contacts made that may result in e-mail being received. IAT reserves the right to monitor all incoming e-mail.
- 2.4 I will communicate with others in a professional manner and only through official communication channels set out in school policies.
- 2.5 Posting anonymous messages and forwarding chain letters is forbidden.
- 2.6 I will ensure that when I take and/or publish images of others I will only do so with their permission and if below the age of 16 with consent of parents/carer and in accordance with the IAT Data Protection Policy on the use of digital/video images. I will not use my personal equipment or the school's equipment (e.g. phone, camera, camcorder or tablet) to record these images, unless I have permission from the CEO/Executive Headteacher/Headteacher/Head of School.) [GB26][AB27]Where these images are published (e.g. on the school or IAT website) it will not be possible to identify by name, or other personal information, those who are featured.

3 All IAT schools have the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- 3.1 When I use my personal hand held/external devices (laptop/tablet/mobile phone etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up-to-date anti-virus software and are free from viruses and have an appropriate level of security to prevent unauthorised use.
- 3.2 I will not use personal email addresses on the school network or IT systems.
- 3.3 I will not open any emails or attachments to emails, unless the source is known and trusted, due to the risk of the attachment containing viruses or other harmful programmes.
- 3.4 I will ensure that my data is regularly backed up, in accordance with relevant IAT policies and that I regularly perform housekeeping on my own network area and any shared drives I am responsible for to ensure files are deleted when no longer needed or archived when no longer in active use.
- 3.5 I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering/security systems in place to prevent access to such materials.
- 3.6 I will not install or attempt to install programmes/apps of any type on the school network or IT systems, or store programmes, nor will I try to alter device settings without permission from the IAT IT MSP Lead.
- 3.7 I will not disable or cause any damage to IAT equipment, or the equipment belonging to others.
- 3.8 I understand that data protection policy requires that any staff or student/pupil



data, to which I have access, will be kept private and confidential, except when it is deemed as necessary that I am required by law or by IAT policy to disclose such information to an appropriate authority.

- 3.9 I understand that if I remove any sensitive data from the school site, I must ensure that this is encrypted by a method approved by the school.
- 3.10 I will immediately report any damage or faults involving equipment or software, however this may have happened, to my line manager and school IT Manager.

4 When using the internet in my professional capacity or for school sanctioned personal use:

- 4.1 I will ensure that I have permission to use the original work of others in my own work.
- 4.2 Where work is protected by copyright, I will not download or distribute copies (including music and videos) without the express permission of the copyright owner.
- 4.3 All computer equipment should be used with care and should be returned in the condition it was leased.
- 4.4 Any equipment that is faulty, missing a part, or malfunctioning must be reported immediately to IT Support.

5 I understand that I am responsible for my actions in and out of school:

- 5.1 I understand that this Acceptable Use Policy applies not only to my work and use of IAT IT equipment in school, but also applies to my use of school network and IT systems and equipment out of school and my use of personal equipment in school or in situations related to my employment by the school.
- 5.2 I understand that if I access school systems whilst offsite (e.g. Arbor, Google Workspace), I am responsible for ensuring I comply with school policy in regard to multi-factor authentication (when required).
- 5.3 I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Trustees and/or the Local Authority and in the event of illegal activities, the involvement of the police.
- 5.4 I understand that teacher's laptops, mobile devices and any desirable items e.g. cameras etc. which are taken off site are my responsibility and they also form part of the school's assets. I am aware that they are not covered by the school insurance when left in a car unattended and if left in an unattended motor vehicle they must be concealed in a locked boot. All school devices must always be kept in a secure place when not in use.
- 5.5 I am responsible for all IT equipment and accessories issued to me and am required to look after, transport and store the equipment effectively in order to prevent damage to the IT equipment and accessories.
- 5.6 I understand that I am liable for any damage caused intentionally or through neglect, to any IT equipment I use and that I am liable for the loss or misplacement of any IT assets that have been assigned to me.
- 5.7 I understand that if any device or data storage device containing school data (e.g. USB memory stick, external hard drive) is stolen it must be reported to the Data



Protection Lead immediately as this is considered a data breach under GDPR.

Staff/Governor/Trustee Acceptance Statement

I confirm that I have read and agreed to abide by these rules and regulations for acceptable use of the IAT IT network and IT systems. I understand that failure to adhere to these rules may lead to my access being revoked and disciplinary measures being taken, including legal action.

Staff Full Name:

Staff Signature: Date/...../.....



Appendix 2: Acceptable Use Agreement (Secondary[AB28] School students)

The school's IT systems are owned by Insignis Academy Trust (IAT) and may be used by all students to further their education. IAT reserves the right to examine, review and delete any files that may be held on its network and computer systems and monitor the visiting of any internet websites or mobile device apps. Students requesting access to the network or/and IT systems need to sign a copy of this Acceptable Computer and Internet Use Policy Statement and return it to the school. Only then will computer and internet access be granted.

Use of IAT IT systems and computers is a privilege, which may be revoked at any time should it be abused.

1 For my personal safety:

- 1.1 I accept personal responsibility for my use of all school IT systems, including but not limited to the following: laptops, Chromebooks, tablets, emails and virtual learning platforms.
- 1.2 The school will monitor my use of the network, computer systems, internet, email and other digital communications. Any evidence of illegal or undesirable activity, for example, cyberbullying, inappropriate language, racism etc, will be dealt with and reported to all appropriate agencies.
- 1.3 The school IT systems are primarily intended for educational use, and I will ensure that no information of a private, personal, or recreational nature is stored on the school network.
- 1.4 Any school username or password will not be disclosed to anybody else, nor will I use the details belonging to another person.
- 1.5 Any illegal, inappropriate, or harmful material or incident must be reported immediately to the IT Support Team and teacher in charge of the lesson.
- 1.6 Any activity that threatens, attacks or corrupts the network or computer systems is forbidden and will be reported to the appropriate agencies.
- 1.7 Any attempt to bypass or interfere with the security systems on the network or computer systems is forbidden and will be reported to the appropriate agencies.
- 1.8 Internet use for financial gain, gambling, political purposes, online purchases or advertising is forbidden.
- 1.9 All computer equipment will be used with care and left in full working order upon completion of work at a computer station or when using a laptop or tablet. No adjustment and/or alternations should be made to computer equipment or the configuration of equipment. If any equipment is faulty or missing or malfunctioning in any way, I will bring it to the attention of the IT Support Team and the teacher in charge of the lesson immediately.
- 1.10 Use of the network and IT systems to access inappropriate material such as pornographic, racist, or offensive material is forbidden and will be reported to all appropriate agencies.

2 I will be responsible in my communications and actions when using school IT systems:



- 2.1 Personal information such as address or phone number should not be given out on the internet, under any circumstances.
- 2.2 I will not take and/or publish images of others in accordance with the school's policy. I will not access, download, remove or otherwise alter any others in accordance with the school's policy. I will not use my personal equipment or the school's equipment (e.g. phone, camera, video camera or tablet) to record images whilst at school.
- 2.3 Access to social network sites, such as Facebook and Instagram is not permitted in school and all access is blocked.

3 Appropriate Use of Artificial Intelligence (AI) in school:

- 3.1 I understand that the use of Artificial Intelligence (AI) tools, such as ChatGPT, Google Gemini, or similar platforms, is permitted for educational purposes only and must adhere to the school's guidelines for academic integrity.
- 3.2 I will not use AI tools to complete assignments or tasks unless explicitly instructed and authorised by my teacher. Any work submitted that is generated by AI without proper acknowledgement and teacher approval will be considered plagiarism and will be subject to disciplinary action.
- 3.3 When permitted to use AI, I will critically evaluate the information provided by AI tools, as they may not always be accurate, unbiased, or complete. I understand that I am responsible for verifying any information obtained from AI.
- 3.4 I will not input any personal or confidential information into AI tools. This includes my own personal details, those of other students or staff, or sensitive school data.
- 3.5 I will use AI tools ethically and responsibly, avoiding the generation of content that is discriminatory, hateful, offensive, or promotes illegal activities.
- 3.6 I understand that the school may use AI detection tools to identify instances of AI-generated content in submitted work.

4 I understand that I am responsible for my actions in and out of school:

- 4.1 I understand that this Acceptable Use Policy applies not only to my work and use of school IT equipment in school, but also applies to my use of school network and IT systems and equipment out of school.
- 4.2 I understand that I cannot take any school electrical equipment off site, without authorisation from the Headteacher/Head of School as they form part of the school's assets. Where permission is granted, it is my responsibility to ensure they are kept safe, secure and returned to the school.

Acceptance Statement

By signing this form, I confirm that I have read and agreed to abide by these rules and regulations for acceptable use of IAT IT network and IT systems, including the guidelines for the use of Artificial Intelligence. I understand that failure to adhere to these rules may lead to my access being revoked and sanctions being applied and, in cases of illegal activity, involvement of all appropriate agencies.

Student Full Name:



Student Signature: Date/...../.....



Appendix 3: Acceptable Use of the Internet – Agreement for Parents and Carers

When communicating with the school via official communication channels, or using private/independent channels to talk about the school, I will:

- 1 Be respectful towards members of staff, and the school, at all times.
- 2 Be respectful of other parents/carers and children.
- 3 Direct any complaints or concerns through the school's official channels.

I will not:

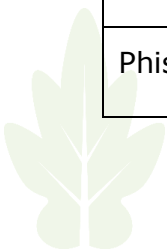
- 4 Use private groups, the school's social media page, or personal social media to complain about or criticise members of staff.
- 5 Use private groups or social media to complain about, or try to resolve, a behaviour issue involving other students.
- 6 Upload or share photos or videos on social media of any child other than my own, unless I have the permission of the other children's parents/carers.



Appendix 4: Glossary of Cyber Security Terminology

This glossary includes key terms to help users understand common forms of cyber-attack and security measures, derived from the National Cyber Security Centre (NCSC) glossary:

Term	Definition
Antivirus	Software designed to detect, stop and remove malicious software and viruses.
Breach	When your data, systems or networks are accessed or changed in a non-authorised way.
Cloud	Where you can store and access your resources (including data and software) via the internet, instead of locally on physical devices.
Cyber attack	An attempt to access, damage or disrupt your computer systems, networks or devices maliciously.
Cyber incident	Where the security of your system or service has been breached.
Cyber security	The protection of your devices, services and networks (and the information they contain) from theft or damage.
Download attack	Where malicious software or a virus is downloaded unintentionally onto a device without the user's knowledge or consent.
Firewall	Hardware or software that uses a defined rule set to constrain network traffic – this is to prevent unauthorised access to or from a network.
Hacker	Someone with some computer skills who uses them to break into computers, systems and networks.
Malware	Malicious software. This includes viruses, trojans or any code or content that can adversely impact individuals or organisations.
Patching	Updating firmware or software to improve security and/or enhance functionality.
Pentest	Short for penetration test. This is an authorised test of a computer network or system to look for security weaknesses.
Pharming	An attack on your computer network that means users are redirected to a wrong or illegitimate website even if they type in the right website address.
Phishing	Untargeted, mass emails sent to many people asking for sensitive information (such as bank details) or encouraging



Term	<u>Definition</u>
	them to visit a fake website.
Ransomware	Malicious software that stops you from using your data or systems until you make a payment.
Social engineering	Manipulating people into giving information or carrying out specific actions that an attacker can use.
Spear-phishing	A more targeted form of phishing where an email is designed to look like it is from a person the recipient knows and/or trusts.
Trojan	A type of malware/virus designed to look like legitimate software that can be used to hack a victim's computer.
Two-factor/multi-factor authentication	Using two or more different components to verify a user's identity.
Virus	Programmes designed to self-replicate and infect legitimate software programs or systems.
Virtual private network (VPN)	An encrypted network which allows remote users to connect securely.
Whaling	Highly targeted phishing attacks (where emails are made to look legitimate) aimed at senior people in an organisation.

