



## **The Inspire Multi-Academy Trust (South West)**

### **Staff and Volunteer Acceptable Use Agreement 2026 - 2027**

This policy is reviewed annually, or as new information becomes available. It is **vital** that this policy is **read** and **understood**.

#### **Purpose and scope**

This agreement sets out the standards expected when using TIMAT devices, accounts, networks, digital services, information and communication technologies. It applies to employees, agency workers, contractors, governors and trustees, volunteers and any other authorised user. In this agreement, "Trust systems" includes equipment, software, email, Microsoft 365, SharePoint, cloud services, networks, internet access, telephony, messaging and any other service supplied or approved by TIMAT. The agreement applies on and off Trust premises whenever Trust systems or information are used, and whenever personal equipment is used on Trust premises or for work connected with TIMAT. It should be read alongside the current versions of the policies listed at the end of this document.

#### **Core expectation**

I will use technology lawfully, safely, professionally and only for authorised purposes. I will protect pupils, colleagues, the Trust and its information and I will report concerns or mistakes promptly rather than trying to conceal them.

#### **1. Responsible and professional use**

- I will use Trust systems primarily for education, safeguarding, administration and other authorised Trust business. Any limited personal use will be reasonable, lawful, infrequent and will not interfere with work, incur avoidable cost or expose the Trust to risk.
- I will act professionally in all digital communications and will not use threatening, abusive, discriminatory, harassing, defamatory or otherwise inappropriate language or content.
- I will not use technology in a way that could reasonably undermine safeguarding, professional boundaries, public confidence in my role, or the reputation of TIMAT or any of its schools.
- I will not access, copy, change, delete or share another user's files or communications unless I am authorised to do so for a legitimate work purpose.
- I understand that devices, accounts, records and data supplied by TIMAT remain the property of the Trust and must be returned or made available when requested.
- I will follow reasonable instructions from the Trust, its schools and authorised IT service providers relating to the safe and secure use of technology.

#### **2. Accounts, passwords and cyber security**

- I will use only the accounts and access rights issued to me. I will not share passwords, authentication codes or security tokens, use another person's account, or allow anyone else to use mine.
- I will use strong, unique passwords and will not reuse a Trust password for a personal account. I will use an approved password manager where one is provided or authorised.
- I will use multi-factor authentication where provided. I will never approve an unexpected sign-in request, disclose a one-time code or bypass an authentication control.
- I will lock my screen whenever I leave a device unattended and will sign out of shared devices when I have finished using them.
- I will not disable or attempt to bypass antivirus, filtering, monitoring, encryption, access controls, updates or any other security measure.
- I will not install software, applications, browser extensions, hardware or services unless they are supplied or approved by TIMAT.
- I will allow required security updates and restarts to complete and will report any device that cannot be updated or appears compromised.
- I will immediately report suspected account compromise, unusual sign-in activity, malware, ransomware, lost or stolen equipment, or any other cyber-security concern using the Trust's agreed reporting route.

#### **Phishing, scams and suspicious communications**

- I will treat unexpected emails, messages, links, QR codes, attachments, requests for payment, requests for credentials and changes to bank details with caution.
- I will not open, respond to or act on suspicious content until I have verified it through a separate, trusted method. A familiar display name or logo is not sufficient verification.
- I will report suspected phishing or fraud promptly. If I have already clicked, replied, entered information or opened an attachment, I will report this immediately and will not try to hide the mistake.

### **3. Personal devices, removable media and equipment**

- I will only use a personally owned device for Trust work where this is authorised and permitted by the Trust's arrangements. Authorisation does not transfer ownership or responsibility for the personal device to TIMAT.
- A personal device used for authorised Trust work must have current security updates, an effective screen lock, encryption and appropriate malware protection. It must not be rooted, jailbroken or shared with unauthorised users.
- I will not store Trust personal or confidential information locally on a personal device, copy it to personal cloud storage, or synchronise it with a personal email or account.
- I will only use removable storage supplied or expressly approved by TIMAT. Any removable device containing personal or confidential information must be encrypted and password protected.
- I will not connect unknown or personally owned USB devices or other storage media to Trust equipment unless specifically authorised.
- I will take reasonable care of Trust equipment, keep it secure and report damage, faults, loss or theft immediately. I will not leave devices or confidential papers unattended in a vehicle.

### **4. Communication and professional boundaries**

- I will communicate with pupils and parents or carers only through Trust-approved systems and for legitimate professional purposes. Communications will be appropriate in content, tone and timing.
- I will not use personal email, personal social-media accounts, gaming platforms, disappearing-message functions or private messaging services to communicate with pupils.
- I will not initiate or accept social-media connections with current pupils. Any unavoidable pre-existing family or community connection will be declared to the Headteacher or another appropriate senior leader.
- I will maintain appropriate boundaries with former pupils, recognising that safeguarding concerns or an imbalance of power may continue after a pupil has left the school.
- I will not create unofficial pupil, parent or class communication groups. Work-related staff groups must use an approved platform and remain professional and confidential.
- I will not record, livestream or share an online meeting, telephone call or conversation unless this has been authorised and everyone has been appropriately informed.

### **5. Images, video and audio recordings**

- I will only take, store, use or publish photographs, video or audio recordings in accordance with the Trust's approved procedures, privacy notices and recorded preferences or permissions.
- I will use Trust-approved equipment and storage. I will not use a personal device to photograph or record pupils unless this has been specifically authorised for an exceptional situation.
- I will check the intended audience, purpose and retention period before publishing or sharing an image or recording. Names and other identifying information will only be used where authorised and appropriate.
- I will not create, alter or share deceptive, sexualised, humiliating or otherwise inappropriate images, recordings, deepfakes or impersonations involving pupils, families, colleagues or anyone connected with TIMAT.
- I will report any inappropriate or unauthorised image or recording immediately and will not copy, forward or retain it except where instructed for safeguarding or evidential purposes.

### **6. Data protection, confidentiality and information sharing**

- I will access personal and confidential information only where I need it for my role and will use it only for the authorised purpose.
- I will keep pupil, parent or carer, staff and Trust information private and confidential unless disclosure is authorised, required by law or necessary under an applicable Trust policy.
- I will use only Trust-approved systems to create, store, transfer and share information. I will apply encryption or another approved secure-transfer method where required.
- Before sending information, I will check recipients, email addresses, permissions, attachments and any auto-completed addresses. I will use BCC where appropriate and will not expose recipients' contact details unnecessarily.
- I will follow the Trust's retention and secure-disposal arrangements. I will not keep copies "just in case", retain information longer than required or dispose of confidential papers in ordinary waste.
- I will not discuss confidential matters in public places or where I may be overheard, and I will position screens and documents so that they cannot be viewed by unauthorised people.

### **Personal and confidential information includes, but is not limited to:**

- safeguarding, child-protection, allegations and complaint information;
- SEND, EHCP, health, medical and disability information;
- pupil and staff records, contact details and identifiers;
- attendance, behaviour, assessment, attainment and examination information;
- photographs, video and audio recordings;
- financial, payroll, recruitment and disciplinary information;
- passwords, access credentials and security information; and
- criminal-offence information and any other special-category personal data.

### **Report data incidents immediately**

A personal data breach may include information sent to the wrong person, lost paperwork, a lost or stolen device, unauthorised access, accidental publication, inappropriate sharing or any other loss of confidentiality, integrity or availability. I will immediately report actual or suspected breaches to the Data Protection Officer and IT support, and to the Designated Safeguarding Lead where a child may be at risk.

### **7. Internet access, content, copyright and software**

- I will not deliberately access, create, upload, download, store or distribute illegal or prohibited material, including child sexual abuse material, terrorist content, criminally racist or extremist material, or content that is pornographic, violent, abusive, discriminatory or otherwise inappropriate for the setting.
- I will not attempt to bypass filtering or security systems, use unauthorised virtual private networks or proxy services, or help another person to do so.
- If I accidentally encounter illegal, harmful or inappropriate material, I will stop viewing it and report it immediately. I will not copy, print, forward or save it unless specifically instructed by the Designated Safeguarding Lead, police or another authorised person.
- I will respect copyright, licensing and intellectual-property rights. I will only copy, download, adapt, publish or distribute material where this is permitted by the relevant licence, statutory exception or copyright owner, and I will acknowledge sources appropriately.
- I will comply with the terms of the Trust's software, media and subscription licences and will not use Trust systems for unauthorised commercial activity, cryptocurrency mining, gambling or unlawful file sharing.

### **8. Use of generative artificial intelligence**

- I will only use generative AI tools and features that have been approved by TIMAT for the intended purpose.
- I will not enter personal, confidential, safeguarding, SEND, health, assessment, behaviour, employment, financial or commercially sensitive information into an AI tool unless its use for that purpose has been expressly approved by the Data Protection Officer or authorised Trust lead.
- I will not use a personal AI account for Trust information or connect an AI tool to Trust email, files or cloud services unless this has been approved.
- I remain responsible for any AI-assisted work. I will check outputs for accuracy, bias, appropriateness, safeguarding risk, copyright or licensing concerns and invented or misleading information before use or publication.
- I will be transparent about material AI use where required by the Trust, professional standards, assessment rules or the context in which the work is used.
- I will not use AI to impersonate another person, fabricate evidence, make automated decisions about an individual, or create misleading images, audio, video or documents.
- Where I am uncertain whether an AI use is permitted, I will seek advice before entering information or using the output.

### **9. Social media and public online activity**

- I understand that online activity may affect my professional standing and public confidence in TIMAT, even where it takes place outside working hours or through a personal account.
- I will use appropriate privacy and security settings but understand that no online content can be guaranteed to remain private, temporary or under my control.
- I will not disclose confidential information, discuss identifiable pupils or colleagues, publish work-related complaints or respond publicly to complaints on behalf of the Trust unless authorised.
- I may identify TIMAT as my employer on a professional networking platform, but I will not use Trust branding without permission or imply that my personal views represent the Trust.
- I will not post, endorse, like, share or comment on material where doing so could reasonably undermine safeguarding, professional boundaries, equality, dignity, public confidence or the reputation of TIMAT or its schools.
- I will not rely on a "views are my own" statement as protection from the consequences of inappropriate online conduct.
- I will report online harassment, impersonation, threats, safeguarding concerns or the unauthorised publication of Trust information through the appropriate Trust route.

### **10. Remote and off-site working**

- I will use approved systems and secure connections when working away from Trust premises and will avoid unsecured public Wi-Fi unless using an approved secure connection.
- I will take reasonable steps to prevent screens, conversations and documents being seen or heard by unauthorised people, including family members and members of the public.
- I will keep paper records securely locked away and will transport them only where necessary and authorised.
- I will not allow family members, friends or other unauthorised people to use Trust devices or access Trust information.
- When my role or volunteering arrangement ends, or when requested, I will return Trust equipment and information and will remove authorised Trust information from personal equipment in accordance with instructions.

## 11. Monitoring and privacy

Activity on Trust devices, accounts, networks and digital services may be logged and reviewed for safeguarding, cyber security, operational, legal and regulatory purposes and to investigate suspected misuse. Monitoring will be undertaken in accordance with data protection law, the Staff Privacy Notice and relevant Trust policies, and will be limited to what is necessary and proportionate.

- I understand that logs may include internet and filtering activity, email and account activity, authentication records, security alerts, device information, file access and use of Trust-approved cloud services.
- I understand that authorised Trust staff and service providers may access relevant information where this is necessary for support, safeguarding, security, legal compliance or an investigation.
- Nothing in this agreement removes my right to raise a concern or make a protected disclosure through the Trust's Whistleblowing Policy.

## Safer recruitment transparency

As part of its safer recruitment procedures, TIMAT may undertake proportionate online searches of publicly available information relating to shortlisted candidates; any potentially relevant information will be considered fairly and explored with the candidate where appropriate.

## 12. Reporting concerns and responding to incidents

- I will immediately report illegal, harmful, inappropriate or suspicious material, communications or activity to the appropriate person. Safeguarding concerns must be reported to the Designated Safeguarding Lead in line with the Safeguarding and Child Protection Policy.
- Cyber-security concerns must be reported to IT support; personal data incidents to the Data Protection Officer; and concerns about professional conduct to the Headteacher, line manager or another appropriate senior leader.
- If the concern relates to a senior leader, or I do not feel able to use the usual route, I will follow the Trust's Whistleblowing Policy or another appropriate escalation route.
- I will preserve relevant evidence where instructed, cooperate with reasonable enquiries and will not investigate a safeguarding, criminal or cyber incident myself unless authorised.

## 13. Breaches and consequences

Access to systems or equipment may be restricted or suspended immediately where this is necessary to protect children, people, information or the Trust. This is a protective action and does not, by itself, determine the outcome of any subsequent investigation.

- Suspected breaches by employees may be considered under the Trust's Disciplinary Policy and other relevant procedures.
- For volunteers, contractors, agency workers, governors or trustees, a breach may result in access being removed and the placement, contract, appointment or volunteering arrangement being ended or reviewed.
- Where required, matters may be referred to the police, local authority designated officer, Disclosure and Barring Service, Teaching Regulation Agency, Information Commissioner's Office, professional body or another appropriate authority.
- Deliberate concealment, repeated non-compliance or failure to report a serious incident may itself be treated as a serious matter.

## Related Trust documents

This agreement should be read alongside the current versions of:

- Staff Code of Conduct (The TIMAT Way...)
- Online Safety Policy
- Safeguarding and Child Protection Policy
- Data Protection Policy and Staff Privacy Notice
- Cyber Security Policy
- Disciplinary Policy
- Whistleblowing Policy

## Declaration

I confirm that I have read and understood this agreement. I agree to use Trust systems, information and my own authorised devices in accordance with these requirements (both in and out of school). I understand that I should seek advice where I am unsure and that failure to comply may result in access being restricted and other action being taken under the relevant Trust procedures.

Staff/Volunteer Name: .....

Signed: .....

Date: .....