EMBARK FEDERATION

Love Learning, Love Life.



Our school is part of the Embark Federation.

The shared vision for our trust is to "create schools that 'stand out' at the heart of their communities." Our trust has four core beliefs; Family, Integrity, Teamwork and Success that are integral to everything we do. The purpose is to enable everyone to be able to 'Love Learning, Love Life.'

Our policies are underpinned by our vision, beliefs and purpose.

Acceptable Use of IT Policy

Date of Issue	01/09/2026
Date of Review	01/09/2027
Version	V4
Approval Level	CEO

Change History
Added Pg 13 - Filtering and monitoring arrangements also extend to the use of Artificial Intelligence (AI).
Wider scope and clearer accountability. Expanded application to employees, trustees, governors, members, volunteers, agency and supply staff, trainees, apprentices, students on placement, contractors, consultants and suppliers. Clarified that the policy applies on and away from Trust premises, including use of personal devices for Trust purposes.
KCSIE 2026 alignment. Updated the statutory context, strengthened online safeguarding expectations, reflected the requirement for all staff to read Part One, and aligned terminology for the making or sharing of nudes and semi nudes, including digitally manipulated and AI generated images.
Cyber security requirements strengthened. Added clearer requirements for account security, strong unique passwords, multi factor authentication, phishing, suspicious messages, device locking, security updates, removable media and attempts to bypass technical controls.
Immediate reporting and supportive reporting culture. Added clearer routes and timescales for reporting cyber incidents, data breaches, lost devices, misdirected information and suspicious activity. Reinforced prompt, honest reporting and the distinction between genuine mistakes and concealment or unnecessary delay.
Data protection and information handling updated. Added the Data (Use and Access) Act 2025, clarified approved storage locations, secure sharing, Bcc use, personal cloud and email restrictions, retention expectations and the process for introducing new uses of personal data.
Artificial intelligence requirements significantly expanded. Introduced approved tool requirements, restrictions on entering personal data, human checking of outputs, professional accountability, safeguards around decision making, AI generated images, transcription and pupil use.
Communication with pupils and parents or carers strengthened. Clarified that Trust approved accounts, platforms and telephone arrangements must be used and that personal email, mobile numbers, messaging apps and social media accounts must not be used for routine school communication.
Mobile phones, cameras and images updated. Added clearer expectations for personal phone use while responsible for pupils, use in toilets and changing areas, educational visits, photography, image storage and briefing visitors, contractors and volunteers.
Filtering and monitoring strengthened. Clarified the annual review of effectiveness, involvement of the responsible senior leader, DSL and IT support, checks across internet connected devices and relevant locations, and the need to keep a record of the review.
Safeguarding and Prevent requirements expanded. Strengthened reporting expectations for online safeguarding concerns, low level concerns about adults, radicalisation, harmful online content and AI related safeguarding risks.
Monitoring, audit and privacy clarified. Set out the types of Trust system activity that may be monitored, the purposes of monitoring, authorisation for individual review and the relationship with the Data Protection Policy and staff privacy notice.
Remote and hybrid working and work life balance strengthened. Clarified expectations for privacy when working away from Trust premises, safe use of online meetings, recording, public WiFi and reasonable expectations for communication and response outside normal working arrangements.

Change History
Changing role or leaving the Trust added. Introduced requirements for reviewing access, returning equipment, transferring and deleting Trust data where appropriate, supporting handover and maintaining confidentiality after employment ends.
Annual declaration and acceptance strengthened. Added an annual renewal requirement and clearer confirmation of staff responsibilities for monitoring, safeguarding, cyber security and data breach reporting.
Management guidance retained and updated. Added guidance for Headteachers and school leaders on induction and annual reminders, supporting staff experiencing online abuse or harassment, preserving evidence, avoiding inappropriate public exchanges, escalation routes and out of hours safeguarding communications.

Contents

1. Purpose
2. Scope and application
3. Your core commitments
4. Safe, responsible and legal use
5. Accounts, passwords and multi-factor authentication
6. Devices and physical security
7. Software, apps and new digital tools
8. Data protection and information handling
9. Email
10. Internet use, filtering and monitoring
11. Artificial intelligence
12. Communicating with pupils and parents or carers
13. Mobile phones, cameras and images
14. Social media
15. Online meetings, remote and hybrid working
16. Safeguarding, Prevent and reporting concerns
17. Reporting cyber incidents and data breaches
18. Monitoring, audit and your privacy
19. Changing role or leaving the Trust
20. Breaches of this policy

Appendix A — Email and messaging etiquette

Appendix B — Who to tell, and how quickly

Appendix C — Declaration and acceptance

Appendix D — Guidance for Headteachers and school leaders

1. Purpose

Embark Federation wants every colleague to be able to work in a digital environment that is safe, secure and effective. Technology is central to how we teach, how we run our schools and how we care for the children in them — and it is also one of the most significant risks the Trust manages. Education is consistently among the most targeted sectors in the UK for cyber attack, and the great majority of successful attacks begin with something a person does rather than something a system fails to do.

This policy sets out what the Trust expects of you when you use its digital tools, technologies, data and resources, and what you can expect of the Trust in return. It is written to be read and used, not filed. If anything in it is unclear, or if it appears to prevent you doing your job properly, please raise it with your line manager or ICT Support rather than working around it.

> **THE SINGLE MOST IMPORTANT LINE IN THIS POLICY**
> If you think something has gone wrong — a device lost, a link clicked, an email sent to the wrong person, a child at risk — report it immediately. You will not be blamed for reporting promptly and honestly. Delay causes far more harm than the original mistake.

2. Scope and application

This policy applies to everyone who accesses Embark Federation systems, data or devices, including:

- employees of the Trust, whether permanent, fixed-term, full-time or part-time
- trustees, governors and members
- volunteers, including parent helpers and governors' visits
- agency, supply and peripatetic staff
- trainee teachers, apprentices and students on placement
- contractors, consultants and third-party suppliers with access to Trust systems

Throughout this policy, "you" and "staff" mean all of the people listed above. "The Trust" means Embark Federation. "Devices" means anything that can access Trust systems or data, whether owned by the Trust or by you personally.

The policy applies:

- on Trust premises and off-site, including at home, on school trips and while travelling
- during and outside working hours
- on Trust-owned devices and on your own devices where these are used for Trust purposes
- to anything you do online that could reasonably affect the Trust, its pupils, or your ability to work with children — including on personal social media accounts

You must read this policy and sign the declaration as part of the Staff Code of Conduct, and again each academic year. New starters complete it as part of induction.

3. Your core commitments

This is the summary. The rest of the policy explains each point in detail. By signing the Code of Conduct you agree to all of it, not only this list.

- **Use technology safely, responsibly and legally.** Take personal responsibility for how you use Trust systems, devices and data.
- **Report concerns without delay.** Any concern about the use of technology by a pupil, member of staff, parent or carer goes to the Designated Safeguarding Lead immediately. Any suspected cyber incident or data breach goes to ICT Support and the Data Protection Officer immediately.
- **Protect your accounts.** Use a strong, unique password, keep multi-factor authentication enabled, and never share your credentials with anyone — including colleagues and ICT staff.
- **Lock it when you leave it.** Any device with access to Trust systems or data must be locked whenever it is not being actively used, however briefly.
- **Keep Trust data in Trust systems.** Store work in the Trust's approved network and cloud locations. Do not move personal data onto local drives, removable media, personal accounts or unapproved third-party services.
- **Do not install or modify.** Only the Trust ICT team may install or change software or hardware on Trust devices, or approve a new digital tool for use with pupils or Trust data.
- **Keep devices updated.** Restart — not shut down — Windows devices at least once a week so that security updates apply.
- **Look after the equipment.** Trust devices are expensive and hard to replace. Secure them, treat them carefully, and report faults, loss or damage to ICT Support immediately.
- **Communicate through Trust channels.** All contact with pupils and with parents or carers uses Trust-approved accounts and platforms — never your personal phone number, email address or social media.
- **Use AI with care and never with personal data.** Generative AI may only be used in line with Section 11. Never enter pupil, staff or family personal data into an AI tool that has not been approved by the Trust.
- **Accept that use is monitored.** The Trust filters and monitors its systems to keep children and data safe. Files and messages held on Trust systems are the property of the Trust.
- **Remember the wider policies.** Your use of technology is also governed by the Trust's Child Protection and Safeguarding Policy, Online Safety Policy, Data Protection Policy and Staff Code of Conduct.

4. Safe, responsible and legal use

Technology is used across the Trust in both administrative and teaching contexts. With that use comes an explicit expectation that it is used responsibly — so that the work of our schools is protected, and so that everyone in our community is protected, so far as is reasonably practicable, from harm arising from careless, uninformed or inappropriate use.

4.1 What acceptable use means

Acceptable use means treating equipment with care, keeping it secure, and using it in ways that are lawful and that do not bring you or the Trust into disrepute. The sections that follow set out how this

applies in particular situations. They are not exhaustive: where a situation is not covered, apply the spirit of this policy and, if in doubt, ask before you act.

4.2 General requirements

All users must:

- take full responsibility for their own use of digital technologies, and use them safely, responsibly and legally
- report any concern about the use of technology by a pupil, member of staff, parent or carer to the Designated Safeguarding Lead without delay
- complete the Trust's online safety, data protection and cyber security training when it is assigned, and keep it up to date
- sign this agreement to confirm it has been read, understood and accepted
- understand that breaches may lead to action under the Trust's Disciplinary Procedure, and in serious cases to dismissal, referral to the Teaching Regulation Agency or the local authority designated officer, or criminal prosecution

4.3 Things that are never acceptable

You must not, under any circumstances:

- attempt to disguise or mask your identity when acting for the Trust, or when interacting with Trust employees, systems, pupils or their families
- attempt to bypass, disable or defeat the technical safeguards protecting Trust networks, devices or accounts — including filtering, monitoring, anti-malware, firewalls, device management or multi-factor authentication
- access, or attempt to access, systems, files, records or areas of the network that you have not been authorised to use, even where a technical route to them exists
- use another person's account, or allow another person to use yours
- use Trust systems for personal commercial gain, for private business, or for political campaigning
- create, store, transmit or knowingly access material that is unlawful, obscene, pornographic, extremist, discriminatory, harassing or abusive

Deliberate attempts to circumvent technical controls may constitute an offence under the Computer Misuse Act 1990 and will be treated as gross misconduct.

4.4 Reasonable personal use

The Trust recognises that a rigid ban on any personal use is neither realistic nor helpful. Limited, occasional personal use of Trust devices and internet access is permitted, provided it:

- takes place outside directed time, and never during teaching, supervision or duties involving pupils
- does not interfere with your work or that of colleagues
- does not incur cost to the Trust or consume significant network capacity
- does not involve anything prohibited elsewhere in this policy
- does not involve storing significant volumes of personal files, photographs or media on Trust equipment

Personal use is a concession, not an entitlement, and may be withdrawn. Anything you do on Trust systems, including personal use, is subject to monitoring under Section 18 and carries no expectation of privacy.

4.5 Compliance audits

The Trust carries out regular audits of compliance with this policy. Where an audit indicates non-compliance, further investigation may follow. Audit findings are reported to the Trust Senior Leadership Team and the Finance and Operations Committee on a termly basis.

5. Accounts, passwords and multi-factor authentication

Your account is the front door to the Trust's information about your colleagues, our pupils and their families. Almost every serious incident in the education sector begins with a compromised account.

5.1 Your account

- You will be issued with a unique username and password through the Trust's account authorisation process. Accounts are personal to you and must never be shared.
- You must change any temporary password at first log-on.
- You are accountable for all activity carried out under your account.
- You must only request or accept the level of system access your role requires. If your access appears to exceed what you need, tell ICT Support.

5.2 Passwords

The Trust follows National Cyber Security Centre guidance. Length and unpredictability matter far more than forced complexity.

- Passwords must be at least [12] characters. The recommended approach is three random words, optionally with numbers or symbols added — for example a memorable but nonsensical phrase.
- Do not base a password on anything guessable or discoverable: names, your school, pet names, dates of birth, telephone numbers, or simple keyboard patterns.
- Do not re-use a Trust password on any other system, and never re-use a personal password for work.
- Change your password immediately, and tell ICT Support, if you suspect it may have been seen, guessed or compromised — including if you have used the same password on a service that has suffered a breach.
- Do not store passwords in a browser's built-in "remember password" prompt on a shared or personal device.
- You may — and are encouraged to — use the Trust's approved password manager, to generate and store credentials. No other password manager may be used for Trust accounts.
- Do not write passwords down and leave them where they could be found, and do not record them in an unprotected file, notebook or phone note.

CHANGE FROM THE PREVIOUS POLICY

> The Trust's ICT team will never ask you for your password, and you must never give it to them or to anyone else. Where ICT Support needs access to your account or device to resolve a problem, they will use an administrative or remote support tool. If anyone asks you for your password — by email, telephone, message or in person — treat it as an attempted attack and report it to ICT Support immediately.

5.3 Multi-factor authentication

Multi-factor authentication (MFA) is required on all Trust accounts where it is available, in line with the DfE cyber security standards. It is the single most effective protection against account compromise.

- You must enrol in MFA when prompted and keep it active. Requests to be exempted must be made in writing to the Chief Operating Officer and will only be granted where there is no workable alternative.
- Approve an MFA prompt only when you have just tried to sign in yourself. If you receive a prompt you did not trigger, deny it and report it to ICT Support straight away — it means someone else has your password.
- Never approve an MFA prompt on behalf of somebody else, and never read a verification code out to anyone.
- Tell ICT Support promptly if the device you use for MFA is lost, replaced or repaired.

6. Devices and physical security

You have a clear responsibility not to jeopardise the integrity, performance or reliability of Trust equipment, software, data and stored information.

6.1 Looking after Trust equipment

- You are responsible for the physical security of any device issued to you. Report faults, loss, theft or damage to ICT Support immediately — and, where a device held Trust data, also to the Data Protection Officer.
- Do not leave IT equipment unattended in a vehicle at any time, and never in view.
- Keep equipment away from food and drink, and protect it from liquids and other contaminants.
- Avoid drops, impacts and pressure from hard objects; carry laptops and tablets in the case provided.
- Do not attempt your own repairs, upgrades or cleaning beyond wiping a screen with an appropriate cloth.
- Return equipment when asked to do so for maintenance, patching, audit or replacement.

6.2 Locking and unattended devices

Any device with access to Trust systems or data must be locked whenever it is not being actively used — including when you step away from your desk, leave a classroom, or move between rooms. Lock the screen rather than relying on a timeout.

Be aware of who can see your screen. Take particular care when working in shared offices, reception areas, staffrooms, on public transport and in any space where pupils or visitors are present.

6.3 Personal devices used for work

- The Trust accepts no responsibility for the safety, loss or damage of personal devices. They are brought onto Trust premises at your own risk.
- Any personal device used to access Trust tools, systems or data must be protected by a password, PIN or biometric lock, must have up-to-date operating system and security updates, and must be running current anti-malware protection.
- Personal devices used for work must be enrolled in the Trust's mobile device management platform where required, and you must accept the controls this applies.
- Family members and other third parties must not use a device while it has access to Trust accounts or data. Use a separate profile if the device is shared.
- Trust data must not be downloaded or copied from Trust systems onto a personal device unless you have specific permission from the Chief Operating Officer to do so.
- You must tell ICT Support before you sell, recycle, trade in or dispose of a personal device that has been used for Trust work, so that Trust access and data can be removed.

6.4 Removable media and unknown hardware

- Trust data must not be stored on USB drives, memory cards, external hard drives or optical media, whether Trust-issued or personal, unless authorised in writing by the Chief Operating Officer. Where authorised, the media must be encrypted to Trust standard.
- Do not connect USB devices of unknown origin — including promotional drives, gifts and items found on site — to any Trust device. Hand them to ICT Support.
- Do not use unknown public charging points or borrowed cables for Trust devices; use a plug and your own cable.

7. Software, apps and new digital tools

- Only personnel from L.E.A.D. IT Services are authorised to install, remove or modify software, or to add hardware, on Trust devices.
- You must not install software for which the Trust does not hold a valid licence, or which has not been approved by the Director of IT. This includes free and trial software, browser extensions, toolbars, screensavers, streaming or download tools, and games.
- You must not attempt to disable or override Trust-installed protections, including anti-malware, firewalls, device management, filtering and automatic updates.
- To ensure security and other updates apply, restart — using Restart, not Shutdown — your Windows device at least once a week. Weekly, before you leave on a Friday, is a good habit.
- Apply prompted updates promptly on any personal device used for work.

7.1 New tools, websites and apps used with pupils

Signing up to a new online service with a Trust email address, or asking pupils to use one, creates a contract and often a transfer of personal data. It cannot be done informally.

- Before any new app, website, platform or subscription is used with pupils or with Trust data, it must be approved through the appropriate channels at your school (usually Headteacher or SBM) and, where personal data is involved, assessed by the Data Protection Officer. A data protection impact assessment may be required.
- Check the provider's minimum age requirement before pupils are asked to use a service. Many require users to be 13, 16 or 18.
- Do not create accounts on third-party services using a Trust email address for anything other than approved work purposes.
- Do not enter Trust or pupil data into a service that has not been approved, however useful it appears.

8. Data protection and information handling

The Trust and everyone working for it must comply with the UK GDPR and the Data Protection Act 2018. The requirements below apply to information in digital and paper form alike.

8.1 Accessing and sharing information

- Only access confidential, restricted or personal information where you have a legitimate, work-related reason. Curiosity is not a lawful basis, and access is logged.
- Only share personal information with those who have a genuine need for it, and only through approved channels.
- Secure information when it is not being actively used, so that it cannot be read, copied or removed. This applies to paper files, printouts and screens as well as devices.
- Never leave documents containing personal data on printers, desks, in classrooms or in vehicles.
- Classify and label information you create in line with the Trust's information classification scheme, and handle it accordingly.
- Comply with the Trust's Records Retention Schedule; do not keep personal data for longer than necessary.

8.2 Where Trust data must live

- Store all work in the Trust's approved locations: the Embark Federation SharePoint and OneDrive environment.
- Do not store Trust information on local hard drives, personal cloud accounts (including personal OneDrive, Google Drive, Dropbox or iCloud), personal email, or removable media, unless authorised in writing by the Chief Operating Officer.
- Do not forward Trust email or documents to a personal email account, including in order to work at home. Use the Trust's remote access instead.
- Where you introduce a new system, process or use of personal data that is not already covered by the Trust's record of processing activities, contact the Data Protection Officer before you begin. You do not need individual authorisation to carry out the routine processing your role requires.

8.3 Sending information outside the Trust

- Check the recipient before you send. Mis-sent email is the most common cause of data breaches in schools.
- Use blind copy (Bcc) when emailing groups of parents or carers so that addresses are not disclosed to one another.
- Do not send personal data outside the Trust unencrypted.
- Take particular care with special category data — health, safeguarding, ethnicity, religion, sexual orientation — and with anything relating to a child who is looked after, has a social worker, or is subject to a protection plan.
- Share access to documents by link with named recipients rather than by attaching copies, and review sharing permissions periodically.

8.4 Printing, copying and scanning

- Trust reproductive equipment (photocopiers, scanners and multifunction devices) may only be used for Trust purposes, and in ways appropriate to the classification of the information.
- Use secure release printing where available, and collect printing immediately.
- Dispose of paper containing personal data in confidential waste, never in general recycling.

9. Email

The Trust email system exists for educational and business communication. All messages, files, header information and attachments carried by Trust systems are the property of the Trust; they are archived separately from the mail server, are recoverable, may be used in evidence, and carry no expectation of privacy.

9.1 Prohibited use

You must not use Trust email to:

- send or forward objectionable material, including pornography and sexually explicit material or jokes
- engage in conduct that is illegal or that breaches the Trust's Staff Code of Conduct
- send offensive or discriminatory messages relating to race, age, disability, sex, gender reassignment, sexual orientation, religion or belief, pregnancy and maternity, marriage and civil partnership, or any other protected characteristic
- advertise or support unapproved or unlawful activities
- circulate chain letters, junk mail, jokes, large media files or executable files
- exchange gossip, rumour, exaggerated claims or unsubstantiated opinion about the Trust, its schools, colleagues, pupils or families
- send anything that would reflect poorly on the Trust's name, reputation or image
- send or forward personal data outside the Trust without encryption or a secure sharing method
- forge, or attempt to forge, a message, or disguise your identity as a sender
- send messages from another person's account without the account holder's and your line manager's knowledge and permission

- knowingly forward an attachment containing malware

Personal email use must not interfere with your responsibilities — in particular teaching, supervision, and duties at break, lunch and the start and end of the day — and must not take up disproportionate or unwarranted time.

9.2 Phishing and suspicious messages

Most attacks on schools arrive by email.

- Never respond to a message asking for account details, passwords, verification codes, payment details or bank changes. Report it using the Report Phishing button in Outlook or to ICT Support, then delete it.
- Treat unexpected attachments, links and QR codes with caution, including in messages that appear to come from a colleague — sender addresses are easily spoofed and colleagues' accounts are sometimes compromised.
- Be alert to urgency, secrecy and pressure: "do this now", "don't tell anyone", "I'm in a meeting". Requests to change bank details or make an urgent payment must always be verified by telephone using a number you already hold, never one supplied in the message.
- If you think you have clicked a link, opened an attachment or entered your credentials, report it straight away. Speed of reporting is what limits the damage, and you will not be blamed for reporting.

9.3 Offensive or upsetting messages

If you receive an offensive, unpleasant, harassing or intimidating message, tell the ICT Team immediately so that it can be traced, and tell your line manager. Where the content raises a safeguarding concern, tell the Designated Safeguarding Lead. If you wish to raise a complaint about email communications, speak to your line manager in the first instance; the Trust's Grievance Procedure is available if the matter cannot be resolved informally.

10. Internet use, filtering and monitoring

The internet is a rich resource for learning and for the running of our schools. It should be used responsibly and proportionately, and should not detract from your other work.

10.1 Expectations

- Do not access or attempt to access websites that are unlawful, obscene, pornographic, abusive, extremist, or that contain adult material. This list is not exhaustive.
- Do not use anonymising services, VPNs, proxies or alternative networks — including tethering to a personal mobile — to reach content that the Trust's filtering blocks.
- Do not download software, media or files that are unlicensed, pirated or in breach of copyright.
- Respect copyright and licensing in materials you use for teaching and in Trust publications, and give proper attribution.

10.2 If you reach something inappropriate

If an inappropriate website is accessed accidentally, report it to a member of the Senior Leadership Team, who will liaise with the Network Manager / ICT Support. Reporting accidental access is expected and will not be held against you; the report also helps improve filtering for everyone.

Where teaching a topic legitimately requires access to material that filtering blocks, request access in advance through [ICT Support], with the approval of a senior leader. Do not attempt to bypass the block yourself.

10.3 Filtering and monitoring

In line with Keeping Children Safe in Education 2026 and the DfE filtering and monitoring standards, the Trust operates filtering and monitoring systems across its networks and devices. All staff are expected to understand their role, complete the training provided and know how to escalate concerns.

The effectiveness of filtering and monitoring must be reviewed at least once every academic year. At school level, the review will be coordinated by the senior leadership team member with responsibility for filtering and monitoring, supported by the Designated Safeguarding Lead and ICT Support. The review must include checks that filtering is working appropriately on all internet connected devices in all relevant locations, and a record of the checks and any actions arising must be retained. Trust oversight sits with the Trust Designated Safeguarding Lead, the Director of IT and the link trustee for safeguarding.
Filtering and monitoring generate alerts. Where an alert concerns a pupil, it is reviewed by the Designated Safeguarding Lead. Where an alert concerns a member of staff, it is reviewed under Section 18.

11. Artificial intelligence

Generative AI tools — including chat assistants, writing and marking aids, image and voice generators, meeting transcription and AI features built into everyday software — can reduce workload and support teaching. They also carry real risks around data protection, accuracy, bias, copyright and safeguarding. This section applies whenever you use AI in connection with your work, on any device.

11.1 The two rules that matter most

> **NON-NEGOTIABLE**
> Never enter personal data into an AI tool that has not been approved by the Trust. That includes pupil names, work, photographs, assessment data, SEND or medical information, safeguarding information, and information about colleagues or families. Assume anything you type into a public AI tool may be stored, reviewed by a human, or used to train the system. And never let AI output go to a pupil, parent or external body without checking it yourself — you remain professionally accountable for it.

11.2 Approved tools

- Only AI tools approved by the Trust may be used for work, Microsoft Copilot within the Trust tenancy.
- Approved tools have been assessed for data protection, security and age-appropriateness. Free or personal-account versions of the same product are not covered by that assessment and must not be used for work.

- To request approval of a new tool, contact the Chief Operating Officer. Approval requires a data protection assessment where personal data is involved.

11.3 Using AI well

- AI is a drafting aid, not a decision-maker. You must review, correct and take ownership of everything it produces.
- AI tools can fabricate facts, quotations, references and statistics with complete confidence. Verify anything factual before you rely on it.
- Check output for bias, age-appropriateness, curriculum accuracy and tone before pupils see it.
- AI must not be the sole basis of any decision that affects an individual — including assessment outcomes, references, admissions, recruitment, safeguarding judgements, or performance and capability decisions.
- Do not use AI to write safeguarding records, child protection referrals, or reports to external agencies.
- Where AI has made a material contribution to a document that goes to parents, trustees or an external body, say so.
- Do not use AI to generate images or audio of real people, including pupils and colleagues.
- Be aware that AI-generated material may reproduce copyrighted content; check before publishing.
- AI meeting transcription and note-taking tools may only be used where the tool is approved and all participants have been told and have agreed.

11.4 AI and pupils

- Pupil use of AI is governed by the Trust's Online Safety guidance and the age limits of the tool concerned. Many major AI services require users to be 13 or 18.
- Where pupils use AI in assessed work, follow current JCQ requirements on acknowledging AI use and authenticating candidate work.
- AI increases the risk of deepfakes, AI-generated nudes and semi-nudes, and AI companions that simulate human relationships. Concerns of this kind are safeguarding concerns and go to the Designated Safeguarding Lead immediately — see Section 16.

12. Communicating with pupils and parents or carers

Clear boundaries in communication protect children, and they protect you.

- All communication with pupils and with parents or carers must use Trust-approved accounts, platforms and telephone numbers. Never use a personal email address, personal mobile number, personal messaging app or personal social media account.
- Do not give pupils or parents your personal contact details, and do not accept theirs for personal use.
- Communication should take place within reasonable hours wherever possible and should be professional in tone and content.

- Do not communicate with a pupil one-to-one through any channel that is not visible to the Trust. Where individual contact is necessary — for example remote tuition or pastoral support — it must be arranged through the school and recorded.
- Keep communication about pupils factual and professional; assume anything you write may be read by the pupil, their family, a court, or in response to a subject access request.
- Do not use Trust systems to contact former pupils under 18, and exercise professional judgement about contact with former pupils generally.
- Where a parent or pupil attempts to contact you through a personal channel, do not respond substantively; report it to your line manager and, where there is any safeguarding dimension, to the Designated Safeguarding Lead.

13. Mobile phones, cameras and images

13.1 Personal mobile phones

Personal mobile phones must not be used for personal purposes during lessons, while supervising pupils, or at any time when you are responsible for children. This includes calls, messages, social media and photography.

- Personal phones should be stored securely and out of sight during directed time — in a locked drawer, staff locker or bag and never in a pocket while working directly with pupils.
- Personal phones must not be taken into toilets, changing rooms, swimming pool areas or any place where pupils are changing, at any time.
- Urgent personal calls can be taken during breaks in the staffroom or another area away from pupils, or through the school office in an emergency.
- On educational visits and residentials, where a personal phone may be needed for safety or logistics, its use must be agreed in advance with the visit leader and restricted to that purpose. A Trust device should be used for any photography.
- Visitors, contractors and volunteers are subject to the same expectations and must be briefed on arrival.

13.2 Cameras, recording and images of pupils

- Photographs and video of pupils may only be taken on Trust-owned equipment, and must be transferred to the Trust's approved storage and deleted from the device promptly.
- Images of pupils must never be stored on a personal device, personal cloud account or personal social media, at any time and for any reason.
- Check consent before photographing, filming or publishing images of pupils, and check it again before any external use. Consent can be withdrawn.
- Do not use personal storage media, personal cameras, MP3 players or personal devices with photographic capability while carrying out your duties, unless specifically authorised by a senior colleague. Such authorisation must be recorded in writing.
- Recording lessons, meetings or conversations — including covertly — requires the prior agreement of a senior leader and of those being recorded.
- Images and recordings must be retained and deleted in line with the Records Retention Schedule.

14. Social media

14.1 Use on Trust equipment

Trust equipment and networks must not be used to access social networking sites or online forums except where this is for an approved educational or professional purpose, or falls within the reasonable personal use allowance in Section 4.4. Where social media is used professionally, it must not damage your standing or that of the Trust.

14.2 Trust and school accounts

- School or Trust social media accounts may only be created with the approval of the Headteacher and the Trust ICT, and must be registered centrally with named account holders and shared administrative access.
- Accounts must not be run from a personal profile or personal email address.
- Content must comply with consent, safeguarding and data protection requirements, and must not identify pupils by full name alongside their image.
- Comments and direct messages must be monitored, and any safeguarding concern passed to the Designated Safeguarding Lead.

14.3 Your personal social media

What you post personally can affect the Trust and your position within it. Social networking invites informality that can leave users exposed.

- Do not accept or send friend or follow requests to current pupils, or to former pupils under 18, on personal accounts.
- Exercise professional judgement about connections with parents and carers, and be alert to conflicts of interest. Where a pre-existing personal relationship exists, tell your line manager.
- Review your privacy settings regularly and limit what is publicly visible, including tagged photographs and friend lists.
- Do not post anything that identifies you as an Embark Federation employee alongside content that could bring the Trust or a school into disrepute.
- Do not post about pupils, families, colleagues or Trust business, including anything that could identify a person indirectly.
- Do not post photographs taken on Trust premises or on school activities to personal accounts.
- Do not respond publicly to criticism of the Trust or its schools on social media; report it to [the Headteacher or the Chief Operating Officer.
- If you are the subject of online abuse or harassment connected to your work, report it to your line manager — the Trust will support you.

14.4 Online abuse or criticism connected to work

If you are targeted, criticised, harassed or threatened online because of your work, do not become drawn into a public exchange. Preserve relevant evidence, including screenshots, dates, times and account details where it is safe and lawful to do so, and report the matter promptly to your line

manager or Headteacher. Where the content raises a safeguarding concern, report it to the Designated Safeguarding Lead. Where there is a threat of violence or suspected criminal conduct, the school or Trust will consider police involvement and appropriate specialist advice.
The Trust has a duty of care to colleagues and will provide proportionate support to staff who experience work related online abuse. This may include management support, HR advice, wellbeing support, help with reporting content to a platform, communications support and, where appropriate, legal or police advice.

15. Online meetings, remote and hybrid working

- The Trust's requirements for the acceptable use of [Microsoft Teams] must be followed at all times.
- Online meetings involving pupils must use Trust-approved platforms and Trust accounts, must be arranged through the school, and must not be one-to-one unless specifically approved and recorded.
- Dress and conduct in an online meeting should be the same as it would be in school. Consider your background, who else is in the room, and what is visible or audible.
- Do not record a meeting without the knowledge and agreement of participants and, for meetings involving pupils, of a senior leader. Recordings containing personal data are Trust records and must be stored and deleted accordingly.
- When working away from Trust premises, use a private space where your screen and conversation cannot be seen or overheard, and lock your device when you step away.
- Avoid open public Wi-Fi for Trust work. Where you must use it, use [the Trust VPN].
- Do not leave Trust equipment or papers accessible to household members or visitors.

15.1 Work life balance and response expectations

Access to email, Teams, learning platforms and Trust systems outside the workplace does not create an expectation that staff are routinely available outside their normal working arrangements. Other than where a role, emergency arrangement or prior agreement requires it, staff should not be expected to read or respond to messages outside their working day before their next reasonable working period.

School leaders should ensure that digital working does not create unreasonable additional workload or shortened response times simply because systems are accessible remotely. Expectations communicated to pupils, parents and carers should make clear that messages and work submitted outside normal working hours may not receive an immediate response.

16. Safeguarding, Prevent and reporting concerns

Embark Federation has legal duties in respect of the safeguarding and protection of pupils. Nothing in this policy limits your safeguarding responsibilities under Keeping Children Safe in Education or the Trust's Child Protection and Safeguarding Policy.

All staff, including those who do not work directly with children, must read Part One of Keeping Children Safe in Education 2026. This requirement forms part of the Trust safeguarding induction and ongoing training arrangements.

16.1 Your duty to report

- You must report to the Designated Safeguarding Lead, without delay, any communication or content you become aware of that gives rise to a concern about a child's welfare — whatever the source, and whether or not you are certain.
- You must disclose the contents of such a communication to the Headteacher or Designated Safeguarding Lead. These may in turn be shared with statutory partners charged with child protection, as required by law.
- Confidentiality cannot be promised where a child may be at risk. Do not agree to keep a disclosure secret.
- Concerns about the conduct of an adult working with children — including online conduct — must be reported to the Headteacher, or to the Chair of Trustees where the concern relates to the Headteacher, in line with Part Four of Keeping Children Safe in Education. Low-level concerns should also be reported.
- The Trust's Whistleblowing Policy is available where you feel unable to raise a concern through the usual route.

16.2 Online risks to be alert to

Concerns arising online should be treated with the same seriousness as those arising in person. These include, but are not limited to:

- content: harmful, extremist, pro-suicide, self-harm, eating disorder or misinformation material
- contact: adults seeking to groom or exploit children, including through games, direct messages and AI systems that simulate human conversation
- conduct: bullying, harassment, and the making or sharing of nudes or semi nudes, including digitally manipulated and AI generated images
- commerce: gambling, financial scams, and criminal or sexual exploitation online

If you become aware of a nude or semi-nude image of a pupil, do not view, copy, share or forward it. Report it to the Designated Safeguarding Lead immediately and follow their instructions.

16.3 Prevent

Under the Prevent duty, you must report any concern that a pupil, or an adult connected to the Trust, may be at risk of radicalisation or being drawn into terrorism to the Designated Safeguarding Lead. This includes concerns arising from online content, searches or communications.

16.4 Illegal content

If you encounter material that you believe may be illegal — in particular indecent images of children — do not investigate, copy, delete or forward it. Secure the device if it is safe to do so, and report immediately to the Designated Safeguarding Lead and Chief Operating Officer, who will take advice from the local authority designated officer and the police.

17. Reporting cyber incidents and data breaches

The Trust has a legal duty to assess reportable personal data breaches and, where required, to notify the Information Commissioner's Office within 72 hours of becoming aware of them. That clock starts when any member of staff becomes aware — not when the report reaches the Data Protection Officer.

17.1 Report immediately if

- you have sent information to the wrong person, or attached the wrong file
- a device, paper file or removable media containing Trust data has been lost or stolen
- you have clicked a suspicious link, opened an unexpected attachment, or entered credentials into a site you now doubt
- you have approved an MFA prompt you did not trigger, or received one you did not trigger
- you notice unexpected activity on your account — messages you did not send, rules you did not create, files you did not move
- a device is behaving unusually: unexpected pop-ups, files becoming inaccessible, sudden slowness, disabled security software
- you have discovered information you should not have access to, or found data left somewhere it should not be
- you suspect someone else's account may be compromised

17.2 How to report

Contact ICT Support on 01332 861956 and the Data Protection Officer at info@phplaw.co.uk immediately — and always the same working day. Where systems may be compromised, use a telephone rather than email. Do not attempt to fix, delete or conceal the problem yourself, and do not switch off a device that may be affected by ransomware unless instructed: disconnect it from the network instead.

> **NO-BLAME REPORTING**
> Anyone can be caught out — attacks are designed by professionals to be convincing. The Trust will not take disciplinary action against a member of staff for making a genuine mistake and reporting it promptly. It may take action where a mistake is concealed, or where a report is delayed.

18. Monitoring, audit and your privacy

Files stored on systems supplied and managed by the Trust are the property of the Trust. The Trust monitors the use of its systems to safeguard pupils, protect personal data, maintain the security and performance of its networks, and evidence compliance with statutory duties.

Monitoring may include internet and filtering logs, email and message content and metadata, file access and sharing, device management and location data for Trust-issued devices, sign-in and security logs, and use of AI tools within the Trust environment.

- Monitoring is proportionate, is carried out for the purposes above, and is subject to the Trust's Data Protection Policy and the staff privacy notice.

- Routine monitoring is automated. Individual review of a named person's activity requires authorisation from the Headteacher or a member of the Trust Executive and is recorded.
- You should have no expectation of privacy in anything created, stored, sent or received on Trust systems, including personal use permitted under Section 4.4.
- The Trust does not routinely monitor personal devices.
- Monitoring information may be used in disciplinary, safeguarding or criminal proceedings.

19. Changing role or leaving the Trust

- Your access rights will be reviewed and amended when your role changes. Tell ICT Support and HR promptly of any change.
- On leaving, all Trust equipment, accessories, removable media and access credentials must be returned by your last working day.
- Trust data held on any personal device or personal account must be transferred to Trust systems and then securely deleted. You must confirm this in writing to ICT Support.
- Accounts are disabled on your last working day. You will not have access afterwards, so save nothing you need to a personal location — instead, ensure your successor and line manager have access to your work within Trust systems.
- Trust information, including documents, resources and pupil data, remains the property of the Trust. It must not be taken with you, and materials created in the course of your employment belong to the Trust.
- Confidentiality obligations continue after your employment ends.

20. Breaches of this policy

The Trust's aim is to support you to work safely, and most issues are resolved through advice and training. However, breaches of this policy may be dealt with under the Trust's Disciplinary Procedure.

Depending on the seriousness of the breach, the Trust may withdraw access to systems or equipment, require additional training, take formal disciplinary action up to and including dismissal for gross misconduct, refer the matter to the local authority designated officer, the Teaching Regulation Agency, the Disclosure and Barring Service or the Information Commissioner's Office, and report the matter to the police.

Examples of matters likely to be treated as gross misconduct include deliberately bypassing security or filtering controls, accessing or distributing indecent or extremist material, deliberately misusing personal data, sharing account credentials, and concealing an incident or breach.

Appendix A — Email and messaging etiquette

These are expectations of professional practice rather than disciplinary rules, but they make a real difference to workload and to how the Trust is perceived.

- Write well-structured messages with a short, descriptive subject line and clear, concise sentences.

- Consider whether email is the right medium. A short conversation often resolves what an email thread will not.
- Avoid text abbreviations and emoji in communications with parents, carers and external partners.
- Do not write in capitals; it reads as shouting.
- Use Cc and Bcc sparingly and purposefully. Everyone copied should know what, if anything, they are being asked to do.
- Avoid "reply all" unless everyone genuinely needs the reply.
- Assume tone will be read at its worst. If a message is difficult, draft it, leave it, and re-read before sending.
- Respect colleagues' time outside directed hours; use delayed send where your working pattern differs from theirs.
- Check the recipient, the attachment and the thread history before sending — particularly when forwarding.

Appendix B — Who to tell, and how quickly

Situation	Who to tell	When
A concern about a child, arising online or offline	Designated Safeguarding Lead	Immediately, same day
A concern about an adult's conduct towards children	Headteacher (or Chair of Trustees if it concerns the Headteacher)	Immediately, same day
Suspected indecent or extremist material	DSL and Chief Operating Officer. Do not view, copy or forward	Immediately
Phishing or suspicious message	[Report Phishing button] or ICT Support	Immediately
Clicked a link, entered credentials, approved an unexpected MFA prompt	ICT Support, by telephone	Immediately
Lost or stolen device, or lost paperwork	ICT Support and Data Protection Officer	Immediately
Information sent to the wrong person	Data Protection Officer	Same working day
Accidental access to an inappropriate website	A member of SLT	Same day
Equipment fault or damage	ICT Support	As soon as noticed
A new app, website or AI tool you want to use	Chief Operating Officer	Before you use it

Situation	Who to tell	When
A request to store or process personal data in a new way	Data Protection Officer	Before you begin

Key contacts:

Trust Designated Safeguarding Lead	Helen Jefferson – h.jefferson@embarkfed.org.uk
ICT Support	Ictsupport@leaditservices.co.uk
Data Protection Officer	info@phplaw.co.uk
Chief Operating Officer	l.baddiley@embarkfed.org.uk

Appendix C — Declaration and acceptance

The declaration is included as part of the Staff Code of Conduct. The evidence of signed declaration through the online platform will be held on your personnel file. You will be asked to renew this declaration each academic year and whenever the policy is materially revised.

I confirm that:

- I have read and understood the Embark Federation Staff Acceptable Use Policy and Agreement.
- I agree to abide by its requirements when using Trust systems, devices, data and resources, whether on or off Trust premises and whether on Trust or personal equipment.
- I understand that my use of Trust systems is monitored and that files and messages held on them are the property of the Trust.
- I understand that I must report safeguarding concerns to the Designated Safeguarding Lead, and suspected cyber incidents or data breaches to ICT Support and the Data Protection Officer, without delay.
- I understand that breaches of this policy may be dealt with under the Trust's Disciplinary Procedure and, in serious cases, may lead to dismissal, referral to a statutory body, or criminal prosecution.
- I know where to find the related policies listed on page 1, and I understand that this agreement does not replace them.

Appendix D — Guidance for Headteachers and school leaders

D1. Leadership responsibilities

Headteachers and school leaders are responsible for embedding this policy in day to day practice and for ensuring that staff understand how to use technology safely and professionally. Leaders should:

- ensure the policy is covered as part of induction and revisited at least annually, alongside online safety, safeguarding, data protection and cyber security training
- ensure staff know how and where to report safeguarding concerns, cyber incidents, data breaches, inappropriate online content and concerns about the conduct of adults
- respond promptly to harassment, bullying or abuse connected to a colleague's work, whether or not a formal complaint has been made
- support employees who are the subject of online abuse through appropriate Trust procedures and available wellbeing, HR, communications or specialist support
- ensure complaints and allegations are handled fairly, consistently and through the appropriate Trust process
- promote reasonable expectations around digital communication so that technology does not create unnecessary workload or an expectation of constant availability

D2. Preventing and managing inappropriate online comments about the school or staff

Schools should take a proportionate and measured approach where parents, carers, pupils or others post inappropriate, abusive or potentially harmful material about the school, a member of staff, a pupil or another member of the community. The aim is to protect people, preserve evidence, use appropriate complaint and safeguarding routes and avoid escalating the situation through public exchanges.

- make clear to parents, carers and pupils how concerns and complaints should be raised and ensure the Complaints Policy is readily accessible
- use parent information, relevant agreements, handbooks and online safety communications to explain expectations for respectful online conduct and the implications of posting inappropriate material about pupils, staff or the school community
- encourage parents and carers to model safe and respectful online behaviour, including appropriate use of photographs and recordings involving children other than their own
- ensure staff know that they should not respond publicly to criticism or become involved in online arguments about school matters

D3. Responding to a specific incident

Each case will require professional judgement. Where concerns arise, leaders should normally consider the following steps:

- keep the response calm, proportionate and impartial
- preserve relevant evidence such as screenshots, account names, dates and times, while protecting confidentiality and avoiding unnecessary sharing

- establish the facts and maintain an appropriate chronology where the matter is ongoing or may require escalation
- consider whether the content raises a safeguarding concern, an allegation about an adult, a data protection issue, a threat, harassment or suspected criminal conduct, and follow the relevant Trust procedure
- support any member of staff or pupil who has been targeted and explain what action is being taken, taking care not to expose them unnecessarily to harmful material
- where appropriate, invite the person raising concerns to use the normal school communication or complaints route rather than continuing the discussion online
- report threatening, abusive or otherwise prohibited content to the relevant platform where appropriate
- alert the Trust Central Team where an issue may attract wider public or media attention so that communications can be coordinated
- seek HR, safeguarding, data protection, legal or police advice where the circumstances warrant it

D4. Supporting staff affected by online abuse

Leaders should recognise the potential professional and personal impact of online abuse. Support should be tailored to the individual and may include regular management contact, access to Embark wellbeing support, HR advice, support from a professional association or trade union, communications assistance, and signposting to specialist online safety support. Where a colleague is not yet aware of harmful material about them, leaders should consider carefully whether, when and how they should be informed, taking advice where necessary.

D5. Out of hours safeguarding communications

There is no general expectation that staff monitor work accounts outside their normal working arrangements. If a safeguarding disclosure is received outside working hours and the member of staff has not seen it, they cannot act on information they have not received. Once a disclosure is seen, normal safeguarding procedures apply and it must be reported as soon as reasonably practicable. Schools should ensure staff understand any local arrangements for urgent out of hours safeguarding contact and should consider appropriate automated messages or signposting where this would assist pupils and families in an emergency.