DARWEN ST JAMES



Nurturing Ambition
Through a Living Faith

Internet Acceptable Use Policy

Statement of Intent

As a professional organisation with responsibility for safeguarding all staff and pupils within the Trust, Cidari is expected to take all possible and necessary measures to protect personal data and information systems and devices from damage, loss, unauthorised access, infection, abuse, theft, and emerging cyber-threats.

This policy aims to:

- Ensure that all members of our community are safe and responsible users of technology.
- Support staff to become empowered and responsible digital creators and users.
- Ensure staff use resources and technology safely, carefully, and responsibly, maintaining strict system security, robust filtering awareness, and password/credential protection.
- Support staff to be safe and considerate online and foster a respectful and caring community on and offline.

1. Legal Framework

1.1. This policy has due regard to all relevant legislation and statutory guidance, including but not limited to:

- Equality Act 2010
- Education Act 2002 / Education Act 2011
- UK General Data Protection Regulation (UK GDPR)
- Data Protection Act 2018
- Data (Use and Access) Act 2025
- Freedom of Information Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

1.2. This policy has due regard to national guidance, including:

- DfE Statutory Guidance: **Keeping Children Safe in Education (KCSIE)** (including requirements regarding annual filtering/monitoring reviews, AI risk management, and mobile phone usage)
- DfE Guidance: *Generative AI in Education: Product Safety Expectations*
- DfE Guidance: *Meeting Digital and Technology Standards in Schools and Colleges*

1.3. This policy operates in conjunction with the following Trust policies:

- Social Media Policy
- Remote Learning & Homeworking Policy
- Personal Devices & Mobile Phone Policy
- Data Protection Policy
- Safeguarding and Child Protection Policy
- Online Safety Policy
- Staff Code of Conduct
- Staff Wellbeing Policy

1.4. This policy should be read alongside the Acceptable Use Policy for Pupils.

2. Roles and Responsibilities

2.1. The Trust Executive is responsible for:

- Ensuring robust ICT risk management procedures and business continuity plans are maintained.
- Monitoring the use and effectiveness of ICT across all Cidari settings.
- Ensuring annual compliance reviews for technical, security, and digital safety controls are executed.

2.2. The Headteacher and Senior Leadership Team (SLT) are responsible for:

- Ensuring staff, volunteers, parents, and pupils adhere to ICT policies at all times.
- Overseeing arrangements for identifying, evaluating, and managing ICT risks.
- Ensuring the designated SLT member for filtering and monitoring, alongside the Designated Safeguarding Lead (DSL) and IT support, carries out and documents an **annual review of filtering and monitoring system effectiveness**.
- Ensuring DSLs and all staff receive appropriate training on filtering and monitoring procedures, cyber-security, and online safety risks (including generative AI and deepfakes).
- Investigating safety issues raised and referring unresolvable matters to the Trust.

2.3. Line Managers are responsible for:

- Maintaining clear communication regarding procedural changes or system updates.
- Ensuring staff are properly trained to carry out duties safely and securely.
- Offering appropriate support to staff experiencing stress or workload concerns related to ICT.

2.4. Employees are responsible for:

- Using computer systems in a professional, lawful, and ethical manner.
- Following all instructions, training, and supervision regarding safe ICT and data handling.
- Immediately raising concerns, risks, or safety incidents with their line manager, DSL, or IT Support.

3. System Security & Cyber-Safety

3.1. Workplace hardware and software are strictly for authorized educational and trust use. Personal data (e.g., personal photos, non-work financial documents) must not be stored on Trust equipment; the Trust accepts no liability for loss of personal data.

3.2. Downloading, installing, or executing unauthorized software or files is prohibited due to malware, ransomware, and cyber-attack risks. Contact ICT support (service.desk@dataspire.co.uk) for software queries. Staff may be held liable where unauthorized actions lead to a data breach.

3.3. Staff must not alter, bypass, disable, or remove any security software, network compliance tools, antivirus programs, or filtering and monitoring solutions placed on Trust devices.

3.4. Staff must not attempt to circumvent network controls, firewalls, or internet filtering systems.

3.5. Any physical damage, theft, loss of equipment, virus/malware infection, or suspected cyber-incident must be reported immediately to ICT support and the Headteacher.

3.6. Staff are responsible for equipment issued to them and may be charged for loss or damage caused by negligence or misuse (excluding normal wear and tear).

3.7. **Monitoring Notice:** The Trust reserves the right to monitor user activity on Trust systems, devices, and networks in real time. This includes digital monitoring of keystrokes, screen views, search queries, and filtered access attempt logs to safeguard staff and pupils, enforce security, and detect harmful or prohibited content.

3.8. Strong password hygiene and multi-factor authentication (MFA) must be maintained. Credentials must never be shared or written down.

3.9. All devices remain Trust property. Equipment must be returned immediately upon request or prior to an employee's final working day.

4. Data Protection & Information Governance

4.1. Staff must adhere to UK GDPR, the Data Protection Act 2018, and the Data (Use and Access) Act 2025. Personal data relating to pupils, staff, or families must be processed lawfully, fairly, kept secure, and retained only in line with record retention schedules.

4.2. Designated Trust systems (e.g., Cloudschool, SIMS, MyConcern, CPOMS) must be used to record, view, and store personal data to ensure compliance, proper backup, and efficient processing of Subject Access Requests (SARs).

4.3. Emails sent or received on Trust accounts are official records subject to Freedom of Information (FOI) requests and Subject Access Requests (SARs). Communications must remain professional. Avoid placing pupil/staff identifying names in email subject headers.

4.4. Third-party data sharing must be vetted and approved by the Academy Data Protection Lead / Trust Data Protection Officer (DPO) to ensure an executed, compliant Data Sharing Agreement is in place.

4.5. Trust personal data, sensitive files, images, or emails must never be stored on personal (non-Trust) devices.

4.6. Google Workspace (or designated cloud infrastructure) must be used as the primary, secure platform for accessing and sharing work documents.

4.7. Avoid emailing file attachments containing personal data. Use native Google Workspace file-sharing permissions with appropriate access controls.

4.8. Any personal data transmitted externally must be protected via Trust-approved encryption methods.

4.9. USB flash drives and unencrypted external storage devices are strictly prohibited unless specifically authorized and provided by the Trust ICT Lead.

4.10. Pupil photos and videos may only be captured on Trust-owned equipment, must strictly align with stored parental consents, and must be routinely uploaded to approved shared drives and erased from local storage (e.g., iPads).

4.11. Generative AI tools must be used in full compliance with data privacy regulations. Staff **must never** input personal, sensitive, or identifiable pupil/staff data into public or unvetted AI tools.

4.12. Staff must exclusively use assigned Trust email addresses (@cidari.co.uk or official academy domains) for all professional correspondence. Using personal email accounts for Trust business or pupil/parent communication is strictly forbidden.

4.13. Staff must routinely clean inbox folders, deleting routine operational emails of short-term value in line with data minimization guidelines.

5. Safeguarding, Online Safety & Emerging Technology

5.1. Staff must immediately report any illegal, inappropriate, or harmful material, online harassment, or potential safeguarding concern to the Designated Safeguarding Lead (DSL) via established reporting systems.

5.2. Staff must remain vigilant to modern online harms including digitally altered/synthetic media, AI-generated abuse ("deepfakes" / "nudes and semi-nudes"), online misogyny/misandry, extremist material, and cyber-bullying.

5.3. In accordance with national guidance, personal mobile phones must not be used by staff in the presence of pupils or during instructional hours, and pupil mobile phone access is prohibited on school grounds throughout the school day.

6. Professional Standards & Email Wellbeing

6.1. All electronic communications across Trust systems must reflect the highest standards of professional conduct and respect.

6.2. Aggressive, derogatory, or discriminatory language will not be tolerated.

6.3. Staff must remain mindful of recipient wellbeing, working patterns, and workload when sending communications.

6.4. The CC field should only include recipients directly relevant to the topic; avoid unnecessarily copying large distribution lists.

6.5. BCC should be reserved strictly for data protection/privacy compliance (e.g., external mass mailings) and never used as an undercover operational escalation tactic.

6.6. Staff should utilize email scheduling features to ensure messages arrive during standard working hours, avoiding disturbance during evenings, weekends, or scheduled holiday periods.

6.7. WhatsApp or equivalent personal messaging applications must not be used for official operational decision-making, attendance updates, or sharing pupil/staff data. Google Chat spaces and official Trust platforms must be utilized instead.

7. Social Media

7.1. When using personal social media, staff must not:

- Disclose confidential information regarding pupils, staff, or Trust operations.
- Post comments that could bring the Trust or its academies into disrepute.
- Post derogatory, defamatory, or abusive comments regarding colleagues, pupils, parents, or stakeholders.
- Interact with current pupils or parents via personal social media accounts.

7.2. Official Trust or Academy social media accounts must be formally approved by the Trust COO, assigned a named account owner, and logged on the Trust Social Media Register prior to creation.

8. Staff Declaration

I confirm that I have fully read, understood, and agree to abide by this Acceptable Use Policy.

- I understand this policy applies to my use of Trust equipment, networks, and systems both on and off premises, as well as my conduct on personal devices where related to my employment.
- I understand that failure to comply may result in disciplinary action up to and including dismissal, referral to Trustees, and, where illegal activity is suspected, escalation to law enforcement.