ICT Acceptable Use Policy (Staff)

Including Visitors, Volunteers, Governors & Trustees

Cidari | All Academies | Public

Version 2.0 Published 1st September 2021 | Owner: COO | Next Review 2022

Statement of intent

As a professional organisation with responsibility for safeguarding all staff 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 and theft

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 that staff use resources and technology safely, carefully and responsibly, respecting system security and password security.
- Support staff to be safe and considerate online and create a community that is respectful and caring, on and offline.

Contents

Statement of intent 1

Contents 1

Legal Framework 2

Roles and responsibilities 2

The Trust executive is responsible for: 2

The Headteacher is responsible for: 2

Line managers 3

Employees 3

System Security 3

Data Protection 4

Safeguarding 5

Wellbeing and Standards 5

Social Media 6

Declaration 7

1. Legal Framework

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

- Equality Act 2010
- Education Act 2004
- The General Data Protection Regulation (GDPR)
- Data Protection Act 2018

This policy has due regard to national guidance including, but not limited to, the following:

- DfE (2021) 'Keeping children safe in education'

This policy operates in conjunction with the following Trust and Academy policies:

- Social Media Policy
- Remote Learning Policy
- Personal Devices (Mobile Phones) Policy
- Data Protection Policy
- Safeguarding Policy / Keeping Children Safe in Education
- Online Safety Policy
- Staff Code of Conduct
- Staff wellbeing policy

1.4. This policy should be read in conjunction with the Acceptable Use Policy for Pupils. Those principles apply equally in this policy.

2. Roles and responsibilities

2.1. The Trust executive is responsible for:

- Ensuring that the Trust has robust risk management procedures in place.
- Ensuring that the Trust has a business continuity plan in place, where required.
- Monitoring the use and effectiveness of ICT within Cidari settings.

2.2. The Headteacher is responsible for:

- Ensuring that staff, parents and pupils adhere to the relevant policies at all times.
- Ensuring all required consents are in place.
- Ensuring that there are arrangements in place for identifying, evaluating, and managing the risks associated with ICT use in their settings.
- Ensuring that there are arrangements in place for monitoring and reporting incidents and near misses relating to ICT use in their setting.
- Overseeing that the Academy has the resources necessary to action the procedures in this policy.

- Reviewing the effectiveness of this policy on an annual basis and communicating any changes to staff, parents, and pupils.
- Arranging any additional training which/that staff may require to support this policy.
- Encouraging staff to report hazards and raise concerns.
- Issues concerning safety raised by anyone are thoroughly investigated and, when necessary, further effective controls implemented and communicated to staff.
- Any safety issues that cannot be dealt with are referred to the SLT/ Trust for action.
- Training for staff is identified, undertaken and recorded to ensure that they are competent to carry out their work in a safe manner.
- Safe systems of work are developed and implemented where needed.

2.3. Line managers

Line managers must ensure that:

- Good communication is in place between management and employees, particularly where there are organisational and procedural changes;
- Employees are fully trained to discharge their duties; and
- Where necessary, they look to offer additional support to any employees who are experiencing additional stress or concerns regarding the use of ICT systems.

2.4. Employees

Employees must:

- Use the Trust's computer systems in a professional, lawful, and ethical manner, consistent with the Trust's ethos, national/local guidance and expectations, the law, and relevant policies.
- Follow any information, instruction, training and supervision provided to them regarding the safe and appropriate use of ICT.
- Raise any issues or concerns with their line manager or designated safeguarding lead where applicable.

3. System Security

3.1. Hardware and software provided by the workplace for staff use can only be used by members of staff and only for educational use. Personal accounts or information such as personal photographs, files or financial information should not be accessed or stored on Trust devices and the Trust accepts no liability for loss of such data.

3.2. Downloading or accessing programmes or files that have not been authorised by IT system managers could result in the activation of malware or ransomware when devices are reconnected to trust networks. If in doubt, staff should contact ICT support for guidance (service.desk@dataspire.co.uk). Where there is a resultant data breach, staff may be individually liable for such a breach.

3.3. Staff must not remove or attempt to inhibit any software placed on trust devices that is required by the Trust for network compliance or security.

3.4. Staff must not attempt to bypass any filtering and/or security systems put in place by the Trust.

3.5. Damage or loss of a computer, system or data including physical damage, viruses or other malware must be reported to the trust's ICT support as soon as possible.

3.6. Staff are liable for any loss, theft or damage to equipment whilst it is in their care and may be charged for any such damage unless it can be attributed to reasonable wear and tear. The Trust can provide details of the value of the equipment for any personal insurance purposes

3.7. The Trust reserves the right to monitor the activity of users on Trust systems and Trust devices from time to time. This includes real-time, digital monitoring of both keystrokes and screen views of harmful content and filtered access to restricted internet sites.

3.8. Password security is important. Get Safe Online provides guidance on password security and recommended Do's and Don'ts https://www.getsafeonline.org/protecting-yourself/passwords

3.9. Equipment remains the property of the Trust. The Trust may request the return of any equipment for any reason at any time by giving appropriate notice. If you leave the employment of the Trust, staff must return equipment prior to the leaving date.

4. Data Protection

4.1. Staff must be aware of their responsibilities under Data Protection legislation (including GDPR) regarding personal data of pupils, staff or parents/carers. This means that all personal data must be obtained and processed fairly and lawfully, kept only for specific purposes, held no longer than necessary and kept private and secure with appropriate security measures in place, whether used in the workplace, hosted online or accessed remotely. This includes safe and secure back up.

4.2. Staff should seek to use designated trust software such as Cloudschool, SIMS, My Concern, or other proprietary software to store, manage, process or view personal information wherever possible to ensure security of information, appropriate deletion and archiving, and to ensure that searches in response to Subject Access Requests can easily and readily be completed.

4.3. Emails created or received as part of your trust job may be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under the Data Protection Act 2018. All Emails should be written and checked carefully before sending, in the same way as a letter written on Academy/ Trust headed paper. Avoid using pupil/ staff names in email headers. All electronic communications with pupils, parents, outside agencies and staff must be compatible with the professional role of staff. The person about whom an email relates may request copies of the information therein.

4.4. Staff are reminded that any sharing of data with third parties should be subject to scrutiny by the academies Data Protection Lead, and if required the Trust Data Protection Officer to ensure an appropriate GDPR compliant data sharing agreement and appropriate licencing are in force.

4.5. Staff must not keep trust-related personal information, including sensitive information, images, files, videos or emails, on any non-trust issued devices.
4.6. Staff should use Google Workspace to access and share work documents and files in a password protected environment.
4.7. Sending copies of data (for example by attachment to email) should be kept to a minimum. Data access to files and folders should be by granting access through the sharing functionality provided within Google Workspace.
4.8. Any data being removed from any Trust site (such as via email) must be suitably protected. This may include email/ data being encrypted by a method approved by the Trust.
4.9. Staff are not permitted to use USB sticks unless approval has been granted by the Trust ICT lead for technical reasons and such devices are encrypted.
4.10. Any images or videos of pupils must only be for official trust use and reflect parental consent. Staff should ensure photos and videos are regularly uploaded to a shared network or official cloud drive, regularly deleted in line with retention policies, and removed from standalone devices such as iPads.
4.11. Staff are expected to respect copyright and intellectual property rights.
4.12. Staff must use trust provided email accounts for all official communication, to minimise unsolicited or malicious email and to ensure all personal data is processed securely. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary Email histories can be traced. The trust email account should be the account that is used for all trust business. Under no circumstances should staff contact pupils, parents or conduct any trust business using personal Email addresses
4.13. Staff should actively manage Email accounts, delete emailsEmail of short-term value and carry out frequent house-keeping on all folders and archives.
4.14. Staff should make full use of enhanced settings provided through Gmail including confidentiality settings, automatic expiry of emails.
4.15. Sharing personal, sensitive, confidential or classified information should only be through Google Workspace, or approved third party secure email systems.
4.16. Staff must be mindful of their duties under Data Protection when working from home and should be familiar with the Trust's Homeworking Policy.

5. Safeguarding

5.1. Staff are expected to immediately report any illegal, inappropriate or harmful material or incidents they become aware of, to the Designated Safeguarding Lead.
5.2. Queries or questions regarding safe and professional practice online either on or off site should be raised with the Designated Safeguarding Lead or the Head teacher.

6. Wellbeing and Standards

6.1. All communication through Trust systems must be carried out in a professional manner.
6.2. As a Trust we are proud to have diversity of thought and individuals will have differing opinions. Aggressive or inappropriate language will not be tolerated.

6.3. When sending emails or other forms of communication, staff should be mindful of the recipient at all times. This may include:

- Their working hours.
- Their availability.
- Their workload.
- Their role and responsibilities in relation to your communication.

6.4. The use of CC and BCC should be carefully considered. Our Trust has a culture of openness and transparency.

6.5. When using CC, staff should ensure that all of the recipients are relevant and required to be included in that communication. If you are responding to a CC email, consider whether the full address list is still required for that response.

6.6. The use of BCC should only be used for confidentiality or data protection reasons.

6.7. CC and BCC should never be used as a 'lever' to give status to a communication, or to attempt to elicit a faster response from the main recipient.

6.8. Scheduling of emails can be routinely used to give consideration to the recipient. Staff should not expect to receive emails outside of their working day, and if the sender's own working patterns (or personal choice) do not align with the recipient, emails should be scheduled to arrive at an appropriate time.

6.9. Staff should be mindful of the timing within the day, week, or term when sending emails requiring urgent action/ response, or containing content that may cause the recipient concern or stress. Instead, consider scheduling so that the recipient receives the email when they begin their next working day (this may be different from your next working day), rather than as they are preparing to leave for the end of the day, a weekend or a holiday.

6.10. Staff should consider their emails carefully before sending.

- Is it needed?
- Is it the best method to communicate in that instance (is a telephone call or Google chat message) more appropriate?
- Is it too lengthy - would a short email and sharing a supporting document be more appropriate?

6.11. Social Media

The Trust has a Social Media Policy, however the following core principles are replicated here.

6.12. When using social media sites, staff will not:

- Reveal confidential information about our pupils, staff, the Academy or Trust.
- Engage in activities on the internet which might bring the Trust into disrepute.
- Use it in any way to attack or abuse stakeholders.
- Post defamatory, derogatory or offensive comments on the Internet about colleagues, pupils or the Trust.

6.13. If staff become aware of any abusive, defamatory, derogatory or offensive comments on social media relating to the Trust, our pupils, parents, staff Governors or Trustees, they must bring it to the attention of their Headteacher immediately.

6.14. Unless a core part of their professional role, the Trust strongly advises that staff do not allow themselves to be openly identified on social media.

6.15. It must be clear that information and opinions shared on personal social media pages are not affiliated to the Trust or role of the person posting.

6.16. Personal social media should not be used to communicate with pupils or parents/ carers.

6.17. Official Trust social media accounts must be formally approved by the Trust COO before going live.

6.18. Any official Trust social media account should have a designated owner who is ultimately responsible for all content posted, security and communications related to that account. This person should be named on the Trust social media register.

6.19. The Trust recognises the social benefits that platforms such as WhatsApp provide to staff. WhatsApp groups should remain informal social communication channels and not used as core operational communication or information/ data sharing tools. Google workspace (and through it the Chat rooms function) can provide a similar user experience but within the security of the Trust system.

7. Declaration

I confirm that I have fully read and understood this policy.

I understand that I am responsible for my actions in and out of the workplace:

- I understand that this Acceptable Use Policy applies not only to my work and use of trust ICT equipment in the workplace, but also applies to my use of trust ICT systems and equipment out of the workplace, as well as my use of personal equipment in the workplace or in situations related to my employment by the Trust.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action which could include, but is not limited to, a warning, a suspension, referral to the Trustees and in the event of illegal activities the involvement of the police.

I have read and understand the above policy and agree to use the Trust ICT systems and my own devices within these guidelines.

Academy/ Site	
Name	
Job Title	
Signed	
Date	