



The Dover Federation

For The Arts Multi Academy Trust

ICT and Internet
Acceptable use Policy
and
Code of Conduct



KEEP AS BLANK PAGE

Contents

1. Introduction and aims	1
2. Relevant legislation and guidance	1
3. Definitions	1
4. Unacceptable use	2
5. Staff (including trustees, volunteers, and contractors)	3
6. Pupils	6
7. Parents	7
8. Data security.....	8
9. Internet access	9
10. Monitoring and review	10
11. Related policies	10
Appendix 1: Facebook cheat sheet for staff.....	11
Appendix 2: Acceptable use of the internet: agreement for parents and carers	13
Appendix 3: Acceptable use agreement for older pupils	14
Appendix 4: Acceptable use agreement for younger pupils	15
Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors	16

1. Introduction and aims

ICT is an integral part of the way our Trust works, and is a critical resource for pupils, staff, trustees, volunteers and visitors. It supports teaching and learning, pastoral and administrative functions of the Trust Academies.

However, the ICT resources and facilities used across the Trust academies also pose risks to data protection, online safety and safeguarding.

This policy aims to:

- set guidelines and rules on the use of Trust ICT resources for staff, pupils, parents and trustees;
- establish clear expectations for the way all members of the Trust community engage with each other online;
- support the Trust's policy on data protection, online safety and safeguarding;
- prevent disruption to the Trust through the misuse, or attempted misuse, of ICT systems;
- support the Trust in teaching pupils safe and effective internet and ICT use.

This policy covers all users of our Trust's ICT facilities, including trustees, staff, pupils, volunteers, contractors and visitors.

Breaches of this policy may be dealt with under our disciplinary policy/behaviour policy/staff discipline policy/staff code of conduct.

2. Relevant legislation and guidance

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

[Data Protection Act 2018](#)

[The General Data Protection Regulation](#)

[Computer Misuse Act 1990](#)

[Human Rights Act 1998](#)

[The Telecommunications \(Lawful Business Practice\) \(Interception of Communications\) Regulations 2000](#)

[Education Act 2011](#)

[Freedom of Information Act 2000](#)

[The Education and Inspections Act 2006](#)

[Keeping Children Safe in Education 2020](#)

[Searching, screening and confiscation: advice for Academies](#)

3. Definitions

"ICT facilities": includes all facilities, systems and services including but not limited to network infrastructure, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications or services, and any device system or service which may become available in the future which is provided as part of the ICT service

"Users": anyone authorised by the Trust to use the ICT facilities, including trustees, staff, pupils, volunteers, contractors and visitors

"Personal use": any use or activity not directly related to the users' employment, study or purpose

“Authorised personnel”: employees authorised by the Trust to perform systems administration and/or monitoring of the ICT facilities

“Materials”: files and data created using the ICT facilities including but not limited to documents, photos, audio, video, printed output, web pages, social networking sites, and blogs

4. Unacceptable use

The following is considered unacceptable use of the Trust’s ICT facilities by any member of the Trust community. Any breach of this policy may result in disciplinary or behaviour proceedings (see section 4.2 below).

Unacceptable use of the Trust’s ICT facilities includes:

- Using the Trust’s ICT facilities to breach intellectual property rights or copyright
- Using the Trust’s ICT facilities to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust’s policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the Trust, or risks bringing the Academies into disrepute
- Sharing confidential information about the Academies, its pupils, or other members of the Trust community
- Connecting any device to the Trust ICT network without approval from authorised personnel
- Setting up any software, applications or web services on the Trust network without approval by authorised personnel, or creating or using any program, tool or item of software designed to interfere with the functioning of the ICT facilities, accounts or data
- Gaining, or attempting to gain, access to restricted areas of the network, or to any password-protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust’s ICT facilities
- Causing intentional damage to ICT facilities
- Removing, deleting or disposing of ICT equipment, systems, programs or information without permission by authorised personnel
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language
- Promoting a private business, unless that business is directly related to the Trust
- Using websites or mechanisms to bypass the Trust’s filtering mechanisms

This is not an exhaustive list. The Trust reserves the right to amend this list at any time. The Trustees, CEO and Headteachers will use professional judgement to determine whether any act or behaviour not on the list above is considered unacceptable use of the Trust’s ICT facilities.

4.1 Exceptions from unacceptable use

Where the use of the Trust's ICT facilities is required for a purpose that would otherwise be considered an unacceptable use, exemptions to the policy may be granted at the Headteacher's discretion.

All situations that necessitate the need for breach of acceptable use will have agreement with the Network Manager and Headteacher and a member of the ICT technician team will supervise the session to ensure no vulnerability to our network or systems.

4.2 Sanctions

Pupils and staff who engage in any of the unacceptable activity listed above may face disciplinary action in line with the Trust's policies on behaviour/discipline/staff discipline/staff code of conduct/Safeguarding Policy.

At Astor Secondary School, if a student has been identified as abusing their use of the ICT network and systems, their privileges are revoked, and access denied for a set period of time. A meeting between staff, student and parents will also take place to discuss the misuses and implications. Before the reinstatement of their access rights, the student will be required to sign a new acceptable use agreement.

5. Staff (including trustees, volunteers, and contractors):

Will:

- Read this policy along with related policies for safeguarding and codes of conduct and disciplinary policies for staff (including parents given authorised access for academy purposes);
- Read this policy along with the Code of Conduct for Governance;
- Read this policy alongside the Safeguarding leaflet (volunteers, visitors and contractors);
- Sign Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors.

5.1 Access to Trust ICT facilities and materials

The Trust's Network Manager manages access to the Trust ICT facilities and materials for Trust staff. That includes, but is not limited to:

- Computers, tablets and other devices
- Access permissions for certain programmes or files

Staff will be provided with unique log-in/account information and passwords that they must use when accessing the Trust's ICT facilities.

Staff who have access to files they are not authorised to view or edit, or who need their access permissions updated or changed, should contact the Network Manager.

5.1.1 Use of phones and email

- The Trust provides each member of staff with an email address.
- This email account should be used for work purposes only.
- All work-related business should be conducted using the email address the Trust has provided.

- Staff must not share their personal email addresses with parents and pupils and must not send any work-related materials using their personal email account.
- Staff must take care with the content of all email messages, as incorrect or improper statements can give rise to claims for discrimination, harassment, defamation, breach of confidentiality or breach of contract.
- Email messages are required to be disclosed in legal proceedings or in response to requests from individuals under the Data Protection Act 2018 in the same way as paper documents. Deletion from a user's inbox does not mean that an email cannot be recovered for the purposes of disclosure. All email messages should be treated as potentially retrievable.
- Staff must take extra care when sending sensitive or confidential information by email. Any attachments containing sensitive or confidential information should be encrypted so that the information is only accessible by the intended recipient.
- If staff receive an email in error, the sender should be informed, and the email deleted. If the email contains sensitive or confidential information, the user must not make use of that information or disclose that information.
- If staff send an email in error which contains the personal information of another person, they must inform the Network Manager and Headteacher **immediately** and follow the Trust's data breach procedure.
- **Staff must not give their personal phone numbers to parents or pupils. Staff must use phones provided by the Trust to conduct all work-related business.**
- Staff who are provided with mobile phones as equipment for their role must abide by the same rules for ICT acceptable use as set out in section 4.

The Trust may record in-coming and out-going phone conversations.

When calls are recorded, callers will be made aware and the reasons for doing so.

All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved. Staff should contact the Company Secretary who will provide protocols.

For example, calls may sometimes be recorded when:

- Discussing a complaint raised by a parent/carer or member of the public
- Calling parents to discuss behaviour or sanctions
- Taking advice from relevant professionals regarding safeguarding, special educational needs assessments, etc.
- Discussing requests for term-time holidays

5.2 Personal use

Staff are permitted to occasionally use Trust ICT facilities for personal use subject to certain conditions set out below. Personal use of ICT facilities must not be overused or abused. The Network Manager, Headteacher or CEO may withdraw permission at any time or restrict access at their discretion.

Personal use is permitted provided that such use:

- Does not take place during contact time, teaching hours or non-break time
- Does not constitute 'unacceptable use', as defined in section 4
- Takes place when no pupils are present
- Does not interfere with their jobs, or prevent other staff or pupils from using the facilities for work or educational purposes

Staff may not use the Trust's ICT facilities to store personal non-work-related information or materials (such as personal documents, personal account details, music, videos, or photos).

Staff should be aware that use of the Trust's ICT facilities for personal use may put personal communications within the scope of the Trust's ICT monitoring activities (see section 5.5).

Where breaches of this policy are found, disciplinary action may be taken.

Staff should be aware that personal use of ICT (even when not using Trust ICT facilities) can impact on their employment by, for instance putting personal details in the public domain, where pupils and parents could see them.

Staff should take care to follow the Trust's guidelines on social media (see appendix 1) and use of email (see section 5.1.1) to protect themselves online and avoid compromising their professional integrity.

5.2.1 Personal social media accounts

Members of staff should ensure that their use of social media, either for work or personal purposes, is appropriate at all times. Guidance and best practice forms part of the Safeguarding and Induction Training. See Appendix 1

5.3 Remote access

We allow staff to access the Trust's ICT facilities and materials remotely.

Remote access can be requested and set up procedure provided by the Network Manager.

Staff accessing the Trust's ICT facilities and materials remotely must abide by the same rules as those accessing the facilities and materials on-site. Staff must be particularly vigilant if they use the Trust's ICT facilities outside the Trust and take such precautions as the Network Manager may require from time to time against importing viruses or compromising system security.

Our ICT facilities contain information which is confidential and/or subject to data protection legislation. Such information must be treated with extreme care and in accordance with our data protection policy. www.dfamat.com

5.4 Trust social media accounts

Academy staff utilising social media platforms to represent academy or activities linked to the academy do so only when authorised by the Headteacher or Headteacher. Senior leaders will be given access. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access the account.

The Trust requires schools to set up named moderators and provide the Network Manager with Admin rights to ensure the security settings comply with Privacy and GDPR regulations

The Trust has social media pages linked to the following academies:

- Barton Junior School
- Shatterlocks Infant and Nursery
- Astor Secondary School

The Trust requires schools to set up named moderators and provide the Network Manager with Admin rights to ensure the security settings comply with Privacy and GDPR regulations.

5.5 Monitoring of Trust network and use of ICT facilities

The Trust reserves the right to monitor the use of its ICT facilities and network. This includes, but is not limited to, monitoring of:

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

Only authorised ICT staff may inspect, monitor, intercept, assess, record and disclose the above, to the extent permitted by law and when authorised by the CEO under protocols available through the Company Secretary.

The Trust monitors ICT use in order to:

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

6. Pupils

6.1 Access to ICT facilities

ICT facilities available to pupils:

- Computers and equipment in an academy's ICT suite are available to pupils only under the supervision of staff.
- Specialist ICT equipment, such as that used for music or design and technology must only be used under the supervision of staff.
- Pupils will be provided with an account linked to the Academy's virtual learning environment, which they can access from any device by using the URL provided to them.

- Sixth-form pupils can use the computers independently for educational purposes only.

6.2 Search and deletion

Under the Education Act 2011, and in line with the Department for Education's [guidance on searching, screening and confiscation](#), the Trust has the right to search pupils' phones, computers or other devices for pornographic images or any other data or items banned under Trust rules or legislation.

The Trust can, and will, delete files and data found on searched devices if we believe the data or file has been, or could be, used to disrupt teaching or break data protection or Trust's rules.

6.3 Unacceptable use of ICT and the internet outside of Trust

Academies will sanction pupils, in line with the behaviour policy, if a pupil engages in any of the following **at any time** (even if they are not on Trust premises):

- Using ICT or the internet to breach intellectual property rights or copyright
- Using ICT or the internet to bully or harass someone else, or to promote unlawful discrimination
- Breaching the Trust's policies or procedures
- Any illegal conduct, or statements which are deemed to be advocating illegal activity
- Accessing, creating, storing, linking to or sending material that is pornographic, offensive, obscene or otherwise inappropriate
- Activity which defames or disparages the Trust, or risks bringing the Trust into disrepute
- Sharing confidential information about the Trust, other pupils, or other members of the Trust community
- Gaining or attempting to gain access to restricted areas of the network, or to any password protected information, without approval from authorised personnel
- Allowing, encouraging, or enabling others to gain (or attempt to gain) unauthorised access to the Trust's ICT facilities
- Causing intentional damage to ICT facilities or materials
- Causing a data breach by accessing, modifying, or sharing data (including personal data) to which a user is not supposed to have access, or without authorisation
- Using inappropriate or offensive language

Academies in the Trust will specify any additional expectations for acceptable use of ICT and sanctions linked to breach of the behaviour policy on their websites.

7. Parents

7.1 Access to ICT facilities and materials

Parents do not have access to the Trust's ICT facilities as a matter of course.

However, parents working for, or with, the Trust in an official capacity (for instance, as a volunteer or as a member of a PTA) may be granted an appropriate level of access or be permitted to use the Trust's facilities at the Headteacher's discretion.

Where parents are granted access in this way, they must abide by this policy as it applies to staff.

7.2 Communicating with or about the Trust online

We believe it is important to model for pupils, and help them learn, how to communicate respectfully with, and about, others online.

Parents play a vital role in helping model this behaviour for their children, especially when communicating with the Academies through our website and social media channels.

We ask parents to sign the agreement in appendix 2.

8. Data security

The Trust takes steps to protect the security of its computing resources, data and user accounts. However, the Trust cannot guarantee security. Staff, pupils, parents and others who use the Trust's ICT facilities should use safe computing practices at all times.

8.1 Passwords

All users of the Trust's ICT facilities should set strong passwords for their accounts and keep these passwords secure.

Users are responsible for the security of their passwords and accounts, and for setting permissions for accounts and files they control.

Members of staff or pupils who disclose account or password information may face disciplinary action. Parents or volunteers who disclose account or password information may have their access rights revoked.

The Network Manager will ensure all account passwords are sufficiently secure.

8.2 Software updates, firewalls, and anti-virus software

All Trust ICT devices that support software updates, security updates, and anti-virus products will be configured to perform such updates regularly or automatically.

Users must not circumvent or make any attempt to circumvent the administrative, physical and technical safeguards we implement and maintain to protect personal data and the Trust's ICT facilities.

Any personal devices using the Trust's network must all be configured in this way.

8.3 Data protection

All personal data must be processed and stored in line with data protection regulations and the Trust's data protection policy.

www.dfamat.com

8.4 Access to facilities and materials

All users of the Trust's ICT facilities will have clearly defined access rights to Trust systems, files and devices.

These access rights are managed by the Network Manager when authorised to do so by the Executive Leadership.

Users should not access, or attempt to access, systems, files or devices to which they have not been granted access. If access is provided in error, or if something a user should not have access to is shared with them, they should alert the Network Manager immediately.

Users should always log out of systems and lock their equipment when they are not in use to avoid any unauthorised access. Equipment and systems should always be logged out of and closed down completely at the end of each working day.

8.5 Encryption

The Trust ensures that its devices and systems have an appropriate level of encryption.

Trust staff may only use personal devices (including computers and USB drives) to access Trust data, work remotely, or take personal data (such as pupil information) out of the Trust if they have been specifically authorised to do so by the Headteacher and use of such personal devices will only be authorised if the devices have appropriate levels of security and encryption, as defined and checked by the Network Manager.

9. Internet access

The Trust wireless internet connection is secured. The Trust uses filters provided by EIS Smoothwall.

9.1 Pupils

Students can request access to a dedicated WiFi network for use with their own devices. This network is isolated from normal traffic, but still enforces our 'student' level web filtering.

9.2 Parents and visitors

Parents and visitors to the Trust will not be permitted to use the Trust's wifi unless specific authorisation is granted by the Executive Leadership, Headteacher or Head of School.

Authorisation will only be granted if:

- Parents are working with the Academies in an official capacity (e.g. as a volunteer or as a member of the PTA)
- Visitors need to access the Trust's wifi in order to fulfil the purpose of their visit (for instance, to access materials stored on personal devices as part of a presentation or lesson plan)

Staff must not give the wifi password to anyone who is not authorised to have it. Doing so could result in disciplinary action.

10. Monitoring and review

The Trustees, CEO, Headteachers and Network Manager monitor the implementation of this policy, including ensuring that it is updated to reflect the needs and circumstances of the Trust.

This policy will be reviewed annually.

The Board of Trustees is responsible for approving this policy.

11. Related policies

This policy should be read alongside the Trust's policies on:

- Online safety
- Safeguarding and child protection
- Behaviour
- Staff discipline
- Data protection

Appendix 1: Facebook cheat sheet for staff

Don't accept friend requests from pupils on social media

10 Rules for Trust staff on Facebook

1. Change your display name – use your first and middle name, use a maiden name, or put your surname backwards instead
2. Change your profile picture to something unidentifiable, or if not, ensure that the image is professional
3. Check your privacy settings regularly
4. Be careful about tagging other staff members in images or posts
5. Don't share anything publicly that you wouldn't be just as happy showing your pupils
6. Don't use social media sites during Trust hours
7. Don't make comments about your job, your colleagues, our Trust or your pupils online – once it's out there, it's out there
8. Don't associate yourself with the Trust on your profile (e.g. by setting it as your workplace, or by 'checking in' at a Trust event)
9. Don't link your work email address to your social media accounts. Anyone who has this address (or your personal email address/mobile number) is able to find you using this information
10. Consider uninstalling the Facebook app from your phone. The app recognises wifi connections and makes friend suggestions based on who else uses the same wifi connection (such as parents or pupils)

Check your privacy settings

- Change the visibility of your posts and photos to **'Friends only'**, rather than 'Friends of friends'. Otherwise, pupils and their families may still be able to read your posts, see things you've shared and look at your pictures if they're friends with anybody on your contacts list
- Don't forget to check your **old posts and photos** – go to bit.ly/2MdQXMN to find out how to limit the visibility of previous posts
- The public may still be able to see posts you've **'liked'**, even if your profile settings are private, because this depends on the privacy settings of the original poster
- **Google your name** to see what information about you is visible to the public
- Prevent search engines from indexing your profile so that people can't **search for you by name** – go to bit.ly/2zMdVht to find out how to do this
- Remember that **some information is always public**; your display name, profile picture, cover photo, user ID (in the URL for your profile), country, age range and gender

What do to if...

A pupil adds you on social media

- In the first instance, ignore and delete the request. Block the pupil from viewing your profile
- Check your privacy settings again, and consider changing your display name or profile picture
- If the pupil asks you about the friend request in person, tell them that you're not allowed to accept friend requests from pupils and that if they persist, you'll have to notify senior leadership and/or their parents. If the pupil persists, take a screenshot of their request and any accompanying messages
- Notify the senior leadership team or the Headteacher about what's happening

A parent adds you on social media

You should decline the offer or ignore the message, consider drafting a stock response to let the parent know that you're doing so

You're being harassed on social media, or somebody is spreading something offensive about you

- **Do not** retaliate or respond in any way
- Save evidence of any abuse by taking screenshots and recording the time and date it occurred
- Report the material to Facebook or the relevant social network and ask them to remove it
- If the perpetrator is a current pupil or staff member, our mediation and disciplinary procedures are usually sufficient to deal with online incidents
- If the perpetrator is a parent or other external adult, a senior member of staff should invite them to a meeting to address any reasonable concerns or complaints and/or request they remove the offending comments or material
- If the comments are racist, sexist, of a sexual nature or constitute a hate crime, you or a senior leader should consider contacting the police

Appendix 2: Acceptable use of the internet: agreement for parents and carers

Acceptable use of the internet: agreement for parents and carers

Name of parent/carer:

Name of child:

Online channels are an important way for parents/carers to communicate with, or about, our Trust.

The Trust academies use the following channels:

- Our official Facebook page
- Email/text groups for parents (for Trust announcements and information)
- Our virtual learning platform
- Parental engagement software for educational purposes

Parents/carers also set up independent channels to help them stay on top of what's happening in their child's class. For example, class/year Facebook groups, email groups, or chats (through apps such as WhatsApp).

When communicating with the Trust via official communication channels, or using private/independent channels to talk about the Trust,

I will:

- Be respectful towards members of staff, and the Trust, at all times
- Be respectful of other parents/carers and children
- Direct any complaints or concerns through the Trust's official channels, so they can be dealt with in line with the Trust's complaints procedure

I will not:

- Use private groups, the Academy's Facebook page, or personal social media to complain about or criticise members of staff. This is not constructive, and the Academy can't improve or address issues if they aren't raised in an appropriate way
- Use private groups, the Academy's Facebook page, or personal social media to complain about, or try to resolve, a behaviour issue involving other pupils. I will contact the Academy and speak to the appropriate member of staff if I'm aware of a specific behaviour issue or incident
- Upload or share photos or videos on social media of any child other than my own, unless I have the permission of other children's parents/carers

Signed:

Date:

Appendix 3: Acceptable use agreement for older pupils

Acceptable use of the Trust's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When using the Trust's ICT facilities and accessing the internet in the Trust, I will not:

- Use them for a non-educational purpose
- Use them without a teacher being present, or without a teacher's permission
- Use them to break Trust rules
- Access any inappropriate websites
- Access social networking sites (unless my teacher has expressly allowed this as part of a learning activity)
- Use chat rooms
- Open any attachments in emails, or follow any links in emails, without first checking with a teacher
- Use any inappropriate language when communicating online, including in emails
- Share my password with others or log in to the Trust's network using someone else's details
- Bully other people

I understand that the Trust will monitor the websites I visit and my use of the Trust's ICT facilities and systems.

I will immediately let a teacher or other member of staff know if I find any material which might upset, distress or harm me or others.

I will always use the Trust's ICT systems and internet responsibly.

I understand that the Trust can discipline me if I do certain unacceptable things online, even if I'm not in Trust when I do them.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of Trust staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in the Trust, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 4: Acceptable use agreement for younger pupils

Acceptable use of the Trust's ICT facilities and internet: agreement for pupils and parents/carers

Name of pupil:

When I use the Trust's ICT facilities (like computers and equipment) and get on the internet in Academies, I will not:

- Use them without asking a teacher first, or without a teacher in the room with me
- Use them to break Trust rules
- Go on any inappropriate websites
- Go on Facebook or other social networking sites (unless my teacher said I could as part of a lesson)
- Use chat rooms
- Open any attachments in emails, or click any links in emails, without checking with a teacher first
- Use mean or rude language when talking to other people online or in emails
- Share my password with others or log in using someone else's name or password
- Bully other people

I understand that the Trust will check the websites I visit and how I use the Trust's computers and equipment. This is so that they can help keep me safe and make sure I'm following the rules.

I will tell a teacher or a member of staff I know immediately if I find anything on a Trust computer or online that upsets me, or that I know is mean or wrong.

I will always be responsible when I use the Trust's ICT systems and internet.

I understand that the Trust can discipline me if I do certain unacceptable things online, even if I'm not in the Trust when I do them.

Signed (pupil):

Date:

Parent/carer agreement: I agree that my child can use the Trust's ICT systems and internet when appropriately supervised by a member of Trust staff. I agree to the conditions set out above for pupils using the Trust's ICT systems and internet, and for using personal electronic devices in the Trust, and will make sure my child understands these.

Signed (parent/carer):

Date:

Appendix 5: Acceptable use agreement for staff, trustees, volunteers and visitors

Acceptable use of the Trust’s ICT facilities and the internet: agreement for staff, governance, volunteers and visitors

Name:

When using the Trust’s ICT facilities and accessing the internet in the Trust, or outside the Trust on a work device, I will not:

- Access, or attempt to access inappropriate material, including but not limited to material of a violent, criminal or pornographic nature (or create, share, link to or send such material)
- Use them in any way which could harm the Trust’s reputation
- Access social networking sites or chat rooms
- Use any improper language when communicating online, including in emails or other messaging services
- Install any unauthorised software, or connect unauthorised hardware or devices to the Trust’s network
- Share my password with others or log in to the Trust’s network using someone else’s details
- Share confidential information about the Trust, its pupils or staff, or other members of the community
- Access, modify or share data I’m not authorised to access, modify or share
- Promote private businesses, unless that business is directly related to the Trust

I understand that the Trust will monitor the websites I visit and my use of the Trust’s ICT facilities and systems.

I will take all reasonable steps to ensure that work devices are secure and password-protected when using them outside the Trust, and keep all data securely stored in accordance with this policy and the Trust’s data protection policy.

I will let the designated safeguarding lead (DSL) and ICT manager know if a pupil informs me, they have found any material which might upset, distress or harm them or others, and will also do so if I encounter any such material.

I will always use the Trust’s ICT systems and internet responsibly and ensure that pupils in my care do so too.

Signed:

Date: