An Daras Multi Academy Trust

Acceptable Use Policy (Pupils, Staff and Community) – New and Developing Technologies

The An Daras Multi Academy Trust (ADMAT) Company
An Exempt Charity Limited by Guarantee
Company Number/08156955

Status: Approved	
Recommended	Yes
Statutory	
Version	v1.3
Adopted v1.0	**Jun 2012**
Reviewed	**Feb 2020**
Next Review	**Feb 2022 [awaiting new Cyber security suite of policies]**
Advisory Committee	ADMAT TLA Committee
Linked Documents and Policies	ADMAT Code of Conduct AUP SMART Rules for Pupils ADMAT Child Protection and Safeguarding ADMAT E Safety Policies ADMAT Whistle Blowing Policy ADMAT IT/Computing Policy ADMAT GDPR Policy and procedures

This policy outlines our purpose in providing and ensuring responsible, safe and efficient use of new and developing technologies.

The SMART rules form the basis of the **Acceptable Use Policy (Pupils)**. These rules are discussed with pupils as a part of their e-safety lessons and prior to any opportunities for access to the internet. These rules will also be reinforced and discussed in Key Stage assemblies. A copy of the SMART rules is attached to this policy **(Appendix 1)**.

The SMART rules are displayed in each class and in work areas around Trust sites.

Parents' attention will be drawn to the Acceptable Use Policy (AUP) by newsletter in the first instance and on the school's web site. Our school AUP will be available for parents and others to read on demand.

The **Acceptable Use Policy (Staff and Community)** can also be found attached **(Appendix 2)**

Internet access in school:
The purpose of internet access in the Trust is to raise educational standards, support the professional work of staff and enhance the Trust management, information and business administration systems.

Staff and pupils will have access to:

- Web sites worldwide offering educational resources, news and current events.

In addition, staff will have the opportunity to:

- Access educational materials and examples of good curriculum practice
- Communicate with the advisory and support services, professional associations and colleagues
- Exchange curriculum/admin data with Local Authority (LA), Department for Education (DfE).

Ensuring Internet access is appropriate and safe:
In common with other media such as magazines, books and video, some material available on the internet is unsuitable for pupils. The academy will take every practical measure to ensure that children do not encounter upsetting, offensive or otherwise inappropriate material on the internet. The following key measures have been adopted to help ensure that our pupils are not exposed to unsuitable material:

- SMART rules must be discussed with pupils as a part of their e-safety lessons and prior to any opportunities for access to the internet
- Our internet access has a robust filtering system which is designed to prevent access to material inappropriate for children

- Pupils using the internet will be working on the academy premises and will be under the supervision of an adult always, monitoring software may be used by the responsible adult
- Pupils using school technology out of school hours e.g. after/before school care will be supervised in line with this policy
- Staff will use their professional judgement and check that the sites pre-selected for pupil use are appropriate to the age and maturity of pupils
- SMART rules are posted in any areas of the school where children can access the internet
- The IT Leader will ensure that occasional checks are made on files to monitor compliance with the academy Acceptable Use Policy
- Methods to quantify and minimise the risk of pupils being exposed to inappropriate material will be reviewed in consultation with colleagues from other schools and advice from the LA, our Internet Service Provider, our IT/GDPR SLA provider and the DfE
- Staff for their own safety must not communicate directly with current or past pupils through private email addresses

Viewing Inappropriate Material:
If there is an incident in which a pupil is exposed to offensive or upsetting material, the school will respond to the situation immediately. Responsibility for handing incidents involving children is taken by the IT Leader and the Child Protection Officer/Executive Head Teacher/Head of School and the pupil's class teacher. All teaching staff will be made aware of the incident at a staff meeting if appropriate.

- If one or more pupils discover (view) inappropriate material they have a responsibility to report it to a staff member immediately
- Our priority will be to give them appropriate support. The pupil's parents/carers will be informed and explained the course of action the school has taken. The school aims to work with parents/carers and pupils to resolve any issue
- If staff or pupils discover unsuitable sites the IT Leader will be informed. The IT Leader will report the URL (web address) and content to the Internet Service Provider and the LA; if it is thought that the material is illegal, the site will be referred to the Internet Watch Foundation and the Police.

Maintaining the Security of the School IT Network:
Security is maintained by updating virus protection, the filtering system, and regular maintenance provided by our SLA IT contractors. The wireless network is secured with a network key and is only accessible through school computers.

Using the Internet to Enhance Learning:
Access to the internet is a planned part of the curriculum that enriches and extends learning activities and is integrated into the class schemes of work. As in other areas of their work, we recognise that pupils learn most effectively when they are given clear objectives for internet use. Different ways of accessing information from the internet are used depending upon the nature of the material being accessed and the age of the pupils:

- Access to the internet may be by teacher (or sometimes other- adult) demonstration
- Pupils may access teacher-prepared materials, rather than the open internet
- Pupils may be given a suitable web page or a single web site to access
- Pupils may be provided with lists of relevant and suitable web sites which they may access

- Pupils are expected to observe the SMART rules and are informed that checks can and will be made on files held on the system and the sites they access
- Pupils will be educated in taking responsibility for their own internet access as part of their e-safety curriculum
- Monitoring software may be used by staff when pupils have access to the internet

Using Information from the Internet:
This is a valuable tool for learning.

- Pupils are taught to expect a wider range of content, both in level and in audience, than is found in the school library or on TV
- Teachers ensure that pupils are aware of the need to validate information whenever possible before accepting it as true, and understand that this is even more important when considering information from the internet (as a non-moderated medium)
- When copying materials from the internet, pupils are taught to observe copyright
- Pupils are made aware that the writer of an e-mail or the author of a web page may not be the person claimed

Using email:
Pupils from Year 3 upwards learn how to use an email application and are taught email conventions. Staff and pupils use email to communicate with others, to request information and to share information. Pupils are only allowed to use email once they have been taught the SMART rules and the reasons for these rules.

- Teachers endeavor to ensure that these rules remain uppermost in the children's minds as they monitor children using email
- Pupils will be given individual email accounts from Year 3 upwards specifically and exclusively for school-based use e.g. writing to French pen pals, writing to children in other schools as part of their learning
- In-coming email to pupils will not be regarded as private
- Pupils may have their email messages they compose checked by a member of staff before sending them
- The forwarding of chain emails and letters will not be permitted
- Pupils are not permitted to use email at school to arrange to arrange to meet someone outside school hours

The Trust Web Sites:
Our school websites are intended to:

- Provide accurate, up-to-date information about the school
- Provide pupils with the opportunity to publish their work on the internet for a very wide audience including pupils, parents, staff, local governors, members of the local community and OFSTED compliance checks
- Celebrate good work
- Promote the school

The point of contact on the school website will be the school address, telephone number and email address.
We do not publish pupils' full names.

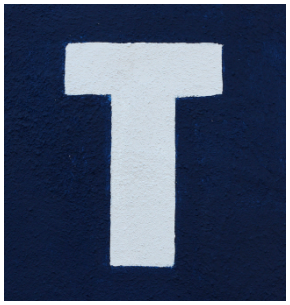
We only use photographs of pupils with parent/carer consent. This consent may be withdrawn at any time but parents/carers must inform the school. Photographs included on the website do not have full names attached to them.

Home information or individual email identities will not be published.

Staff will be identified by their title and surname unless they request otherwise. Permission will be sought from other individuals before they are referred to by name on any pages we publish on our website.

Appendix 1 - Acceptable Use Policy (Pupils)

SMART Rules for Pupils Acceptable Use



Appendix 2 – Acceptable Use Policy (Staff and Community)

Rationale:
This policy details the expectations regarding Trust staff's use of technology. The policy covers expectations for all staff and visitors of the school and contains four strands. This policy is to be adhered to during all Trust school activities on and off the school site.

1. Safety
The main purpose of the policy is regarding safeguarding and to ensure the safety of all pupils and the wider community of the school.

2. Privacy
We welcome and value each member of the Trust community to their right to privacy and as such each member of the community is entitled to choose not to feature in photographs or videos recorded at the school, on and off site.

3. Protecting the Trust's Image
Use of technology at Trust schools or the Trust Central Office should not do anything which may cause any embarrassment to the Trust, the children, parents, carers, staff, visitors or members of the wider school community.

4. Radicalisation and British values
To ensure technology is used positively to promote British values and to inform the community of dangers related to radicalisation.

Changes to permissions
Any failure to adhere to this policy may lead to a withdrawal of permission to use certain technologies at the Trust for a set period.
NB: *Technology refers to computers, laptops, I-pads, tablets, visualizers, photocopiers, cameras, scanners, telephones, mobiles, screens, software, hardware, accessories, internet, social media and any other technology equipment.*

Staff Acceptable Use Policy:
All members of the Trust community are aware of the following expectations:

- That technology includes a wide range of systems, including computers, laptops, iPads, tablets, visualizers, photocopiers, cameras, scanners, telephones, mobiles, screens, software, hardware, accessories, internet, social media and any other technology equipment.
- That it is a disciplinary offence if there is a failure to meet expectations as set out in this policy.
- Staff will ensure they will not disclose any passwords provided to them by the Trust.
- Trust staff and community users understand that they are responsible for all activity carried out under their username.

- Staff, directors/local governors and visitors will not install any hardware or software on any Trust owned device without the prior permission of a member of the senior leadership team, the computing leader or computing technicians.
- That their use of the internet may be monitored and if anything, untoward is un-covered could be logged and used in line with any disciplinary procedures. This includes all Trust owned devices. If an e-safety, safeguarding or GDPR incident should occur, staff will report it to the Trust designated professional for Child Protection and/or the Trust Data Protection Officer immediately.
- Trust community users will use only the school's email/internet/intranet and any related technologies for uses permitted by the Executive Head Teacher/Head of School or local governing body. If anyone is unsure about an intended use, they should speak to the senior school leader beforehand.
- Trust community users will ensure that data is kept secure and is used appropriately as authorised by the Executive Head Teacher/Head of School or local governing body. No passwords should be divulged and if still in use memory sticks should also be encrypted.
- Personal devices must only be used in the context of Trust business with the explicit permission of the Executive Head Teacher/Head of School. Personal mobile phones or digital cameras must NEVER be used for taking any photographs during Trust activities on or off Trust sites.
- Trust community users using Trust equipment will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory or inappropriate.
- Trust community users will use only the approved email system (Office 365) for Trust business.
- Images will only be taken, stored and used for purposes within the Trust unless there is written parental permission for alternative use such publication.
- Trust community users must adhere to the expectations set out in the photography and video policy.
- Trust community users will make every effort to comply with copyright and intellectual property rights.
- Trust community users will report any incidents of concern regarding staff use of technology and/or children's safety or possible GDPR breaches to the Executive Head Teacher/Head of School or to the designated professional in line with the Trust Child Protection and Safeguarding Policy.
- Trust community users will be alert to radicalisation. For example, disclosures by pupils about their exposure, inside or outside of school, to extremist actions, views or materials, accessing extremist material online, voicing extremist opinions and using extremist language and parental reports of changes in pupils' behaviour.
- Trust community users will promote fundamental British values, the Trust will take measures such as: Planning an assembly programme focused around ethical values and beliefs and ensuring the planning of assemblies is focused around ethical values and beliefs and ensuring the school council/forum enables pupils to actively participate in the democratic process.

Staff Technology Expectations Agreement Form:

I acknowledge that I have read and will adhere to the expectations set out in the Trust Acceptable Use of Technology Policy 2020.

Full Name _____

Signature _____

Date _____