Tapton SCHOOL

ACADEMY TRUST

Realising the life chances and dreams of every child

STAFF ACCEPTABLE USE FOR ONLINE SAFETY AND SOCIAL NETWORKING STANDARDS

Date of issue:	July 2023
Originator:	IT Director
Responsible sub-committee:	Risk & Governance Committee
Linked Policies:	Data Breach Policy, Data Protection Policy, ChildProtection & Safeguarding Policy, CCTV Policy
Review Date:	June 2024
Target audience:	All stakeholders in the Trust
Dissemination via:	Email, SharePoint

Updates

Version	Section	Amendments	Date	Author
1.0	Acceptable Use Social Networking Don'ts Title	Edit point 20 to include smart wear. Added point 21 Added point 10 Changed to Online Safety from E Safety	February 2020	L Askin
2.0	Acceptable Use	Add working from home	November 2020	L Askin
3.0	Teams/Online Learning and Meetings	Teams/Online Learning and Meetings section added	February 2021	L Askin
4.0	Acceptable Use	Guidance added on sharing screens	January 2023	L Askin
5.0	Acceptable Use	Guidance on use of dashcams	April 2023	L Askin

Tapton School Academy Trust recognises that the use of ICT, Internet, SharePoint, the Learning Platform and a wide range of electronic communication can greatly enhance the quality of learning across our Trust.

It is vital that everyone adheres to this policy to ensure safe, appropriate and responsible use of such technologies.

Acceptable Use

- I will read and comply with the ***Trust's Data Protection Policy.***
- All data stored by TSAT staff is the property of TSAT and should not be removed when staff leave.
- I will not disclose my username or password to anyone.
- I will not write down or store a password unsecurely.
- I will always log off the computer when I have finished and lock it when unattended.
- I will never use anyone else's login, email address or password.
- When working away from school I will only log into school systems using a secure wi-fi network.
- I will not use my personal email or personal phone number as a contact for students.
- I will never use my personal email address for work.
- When communicating electronically with students or parents it will only be via the school's accredited systems.
- I will ensure that all communication is transparent and open to scrutiny.
- I will ensure that communication with students is in a professional manner.
- I understand that the use of the network or any school device to knowingly access inappropriate materials is strictly forbidden and may constitute a criminal offence.
- I will report any accidental access to unacceptable material immediately to my manager and notify my manager if I suspect someone else of misusing ICT. I will also inform the Designated Safeguarding Lead if misuse may be a child protection issue.
- I will ensure that students under my supervision use ICT facilities and the Internet appropriately to support learning. I will challenge and report any misuse.
- Where I am sharing my screen with others (including whiteboards) I will ensure sensitive / personal data is not shared unintentionally. This can be achieved by using extended desktop or freezing a duplicated display.
- I will ensure the ICT team have screened all devices for malicious software before connecting to the network and take care when opening unknown email attachments. I will seek advice from the ICT team if I am unsure about the safety of any such devices or attachments.
- I will make sure that if I need to transport personal data of any kind I will do so using an encrypted external device that has a password in line with the ***Trust's Data Protection Policy.***
- I will not attach any devices to the network that may contain files that breach copyright, GDPR or other laws.
- I agree to use the school's ICT only for work related use during my directed working hours.

- If I use a work mobile device or laptop at home and in school, I will not access inappropriate applications/ Internet searches (including gambling).
- I will take all reasonable steps to ensure the safety of ICT which I take off site and will remove anything of a personal nature before it is returned to school.
- My mobile device (phones, tablets, smart wear) will be turned off or kept on silent mode during working hours except if required to authenticate with school network login or email, or in an emergency situation with the agreement of a member of the Senior Leadership Team.
- Employees should not access personal emails or messages during directed working hours except in an emergency situation with the agreement of a member of the Senior Leadership Team.
- I will only photograph or video students on school devices as part of a planned learning activity or, in exceptional circumstances, for identification purposes and will ensure footage is only used with the correct consent.
- I will not photograph or video students on personal devices.
- If I choose to have my school email account configured on my personal mobile device, I will set a 6-digit passcode and install the school Microsoft Intune email policy application and accept the agreement**.**
- I understand that the Trust monitors Internet usage and sites used by staff. All inappropriate searches are automatically alerted to the DSL and Headteacher.
- I understand that the misuse of ICT facilities and the Internet could result in disciplinary action being taken.
- I will follow Trust password policy of: At least 8 characters, At least 1 capital letter, at least 1 number.
- When working from home I will not leave any school system logged in unattended, these include remote access, Bromcom, SharePoint and video conferencing meetings or training.
- If I have a dashcam fitted in my car I will ensure that any internal audio recording will be disabled if I am making or receiving work related calls. I will also disable any internal video (if applicable)/audio recording if I am transporting children between locations.

Online Learning and Meetings - including Teams and Zoom

To find out how to do any of the below please visit the Trust Knowledge Base site to access useful guides - https://tsat.sharepoint.com/sites/tsat/policies/KnowledgeBase

- When using Teams always blur your background when providing online lessons, recording online content, or attending a meeting when outside of school.
- When using Zoom for a meeting whilst outside of school always upload and apply a custom background.
- Only use scheduled meetings setup in your Teams/Zoom calendar with students or meeting attendees.
- Make sure you end the meeting when meeting with students (or meetings attendees) and do not just leave.

- Always set the lobby option to 'Only me' (organiser) in Teams and enable the Waiting Room in Zoom for all external meetings and lessons so that you know who you is attending, and you can admit each person to the meeting.
- Always set the who can present option to 'Only me' (organiser) for all lessons with students. In Zoom you need to change the share screen advanced sharing options for who can share to 'Only Host' (organiser). Its optional whether you want to do this for meetings with adults in Teams/Zoom.
- If recording a meeting, always make sure the attendees are aware and they are happy for you to record the meeting, if they are not then do not record. Once you start the recording state that the meeting is being recorded and participants have consented to it. *"Please note that any attempt to covertly record such a meeting may be considered as gross misconduct"*.
- When entering a meeting/lesson you should always seek to ensure that your camera and microphone is active so that the person leading the meeting/lesson is made aware of your presence.
- If there are any issues with the use of camera (i.e., WIFI or data issues) then you should make the person/s leading the meeting/lesson aware of this.
- Any use of message chat should be to appropriately contribute to the meeting/lesson taking place. It should be the person/s leading the meeting who decide if the message chat needs to be shared on the screen to support the meeting.

Staff social networking standards

Below sets out the standards expected of all staff when using social media.

DO

- Always act responsibly. Even if you do not identify your profession or place of work, your conduct could jeopardise any professional registration and/or your employment.
- Be considerate to your colleagues. Pictures or information about colleagues should not be posted on social networking sites unless you have the agreement of the individual.

DO NOT

- Share confidential information online.
- Build or pursue relationships with pupils even when the pupil has left the Trust.
- Use social networking to inform professional practice without careful consideration and discussions with management.
- Discuss students, parents, colleagues, school or Trust in a way which may be deemed inappropriate or damage reputation.
- Post pictures of students/families online even if they have asked you to do this.
- Take pictures of parents, carers, or students without the relevant consents.
- Raise concerns about your work online. If you have concerns, then these should be discussed with

your line manager.

- Engage in activities online which may bring the Trust into disrepute.
- Be abusive, bully, derogatory, defamatory, or offensive.
- Employees may not use social networking sites or other unauthorised sites during directed working hours.

All the above applies to open and private sections of social networking sites.