Policy:	**Acceptable Use Policy and Agreement**
Owner:	Trust IT Lead
Approving Board:	Executive Group
Date of Review:	October 2025
Date of Next Review:	October 2026
Relevant To:	All TDET
Publish status:	SharePoint

Contents

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 2021
- Searching, screening and confiscation: advice for trusts
- National Cyber Security Centre (NCSC)
- Education and Training (Welfare of Children Act) 2021

Purpose and scope

This policy is designed to enable acceptable use for staff.

The trust provides a range of ICT resources which are available to staff members. To ensure the safety of staff and pupils it is important that all staff members follow the guidelines detailed below.

This policy aims to:

- Promote the professional, ethical, lawful and productive use of the trust's ICT systems and infrastructure.
- Define and identify unacceptable use of the trust's ICT systems and external systems.
- Educate users about their data security responsibilities.
- Describe why monitoring of the ICT systems may take place.
- Define and identify unacceptable use of social networking sites and trust devices; and
- Specify the consequences of non-compliance.

This policy applies to staff members and all other regular users of the trust's ICT systems who are expected to read and understand this policy. To confirm acceptance of the policy, users will sign an Acceptable Use Agreement which is attached to this policy. Breach of any part of this policy may result in disciplinary action.

The use by staff and monitoring by the trust of its electronic communications systems is likely to involve the processing of personal data and is therefore regulated by the Data Protection Act 2018, together with the Employment Practices Data Protection Code issued by the Information Commissioner. Staff are referred to the trust's Data Protection Policy for further information.

If you are in doubt and require clarification on any part of this document, please speak to the Trust IT Lead.

Provision of ICT Systems

All equipment that constitutes the trust's ICT systems is the sole property of the trust.

No personal equipment should be connected to or used with the trust's ICT systems. Users must not try to install any software on the ICT systems without permission from IT Services. If software is installed without permission, it may cause extensive damage to the ICT systems and users could be held personally liable for any costs incurred in rectifying the damage.

IT Services are responsible for purchasing and/or allocating ICT equipment to individuals. Individual laptops/desktop computers or ICT equipment may be removed at any time and without prior warning for regular maintenance, reallocation or any other operational reason. Maintenance includes but is not limited to, new software installations, software updates, reconfiguration of settings and computer re-imaging.

Network Access and Security

Users are not permitted to make any physical alteration either internally or externally, to the trust's computer and network hardware.

All users of the ICT systems at the trust must first be registered. Following registration, a network user account will be created consisting of a username, password and an e-mail address. All passwords should be of a complex nature to ensure data and network security. All user account details are for the exclusive use of the individual to whom they are allocated. Staff are responsible for ensuring their password remains confidential and their account is secure. Passwords must be regularly changed.

All users are personally responsible and accountable for all activities carried out under their user account(s). Users must take all reasonable precautions to protect their user account details and must not share them with any other person, except to designated members of IT Services for the purposes of system support. Users must report any security breach or suspected breach of their network, email or application account credentials to a member of IT Services as soon as possible.

Users should only access areas of the trust's computer systems to which they have authorised access.

When any computer is left unattended, it must either be logged off or locked. Activity that threatens the integrity of the trust's ICT systems or activity which attacks or corrupts other systems, is forbidden. Users' internet activity must not compromise the security of the data on the trust's ICT systems or cause difficulties for any other users.

Under no circumstances should a pupil be allowed to use a staff computer account.

Trust Email

Where email is provided, it is for academic and professional use with no personal use being permitted. The trust's email system can be accessed from both the trust computers and via the internet from any computer. Wherever possible, all trust related communication must be via the trust email address.

The sending of emails is subject to the following rules:

- Language must not include swear words, be offensive or abusive.
- Emails or attachments of a pornographic, illegal, violent, sexist or racist nature are not permitted.
- Sending of attachments which contain copyright material to which the trust does not have distribution rights is not permitted.
- The use of personal email addresses by staff for any official trust business is not permitted.
- The forwarding of Trust\School emails to personal email accounts is not allowed. If you need to access school emails when not onsite, log into your school email account on the Trust M365 portal.
- The forwarding of any chain messages/emails etc. is not permitted. Spam or junk mail will be blocked and reported to the email provider.
- Any electronic communication which contains any content which could be subject to data protection legislation (e.g., sensitive or personal information) will only be sent using a secure method including:
    - Email encryption.
    - A secure upload portal (whereby the recipient will be required to log in to retrieve the email/documentation sent).
    - Password protection on sensitive documents. The sender must ensure that the password is sent separately to the intended recipient (i.e., in a separate email or over the phone).

- 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 should not make use of or disclose that information.
- If staff send an email in error that contains personal information of another person, then they must raise a GDPR Breach notification via the trust SharePoint site and contact your local GDPR lead immediately for advice and follow our data breach procedure.
- Emails should not contain children's full names in the subject line and preferably, not in the main body of the text either. Initials should be used wherever possible. Any email containing personal data should be deleted in line with the Data Retention Policy as soon as it has served its intended purpose.
- Access to trust email systems will always take place in accordance with data protection legislation and in line with other appropriate trust policies.
- Members of the community must immediately tell a designated member of staff if they receive offensive communication, and this will be recorded in the relevant files/records (such as safeguarding).
- Staff will be encouraged to develop an appropriate work life balance when responding to email.
- Emails sent to external organisations should be written carefully and checked before sending, in the same way as a letter written on trust or school headed paper would be.
- Trust email addresses and other official contact details will not be used for setting up personal social media accounts.
- Where possible, emails must not contain personal opinions about other individuals e.g., other staff members, children or parents. Descriptions of individuals must be kept in a professional and factual manner.
- 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.

Internet Access

Internet access is provided for academic and professional use with reasonable personal use being permitted. Priority must always be given to academic and professional use.

The trust's internet connection is filtered meaning that a large amount of inappropriate material is not accessible. However, on occasions it may be possible to view a website which is

inappropriate for use in a school. In this case, the website must be reported immediately to IT Services.

Staff must not access from the trust's system any web page, or any files downloaded from the web which could be regarded as illegal, offensive, in bad taste or immoral.

Misuse of the internet may in certain circumstances, constitute a criminal offence. Misuse of the e-mail system or inappropriate use of the internet by viewing, accessing, transmitting or downloading any of the following material or using any of the following facilities will amount to gross misconduct (this list is not exhaustive):

- accessing pornographic material (that is writings, pictures, films, video clips of a sexually explicit or arousing nature), racist or other inappropriate or unlawful materials.
- transmitting a false and/or defamatory statement about any person or organisation.
- inappropriate advertising, phishing and/or financial scams
- sending, receiving, downloading displaying or disseminating material which is discriminatory, offensive, derogatory or may cause offence and embarrassment or harass others.
- transmitting confidential information about the trust and any of its staff, students or associated third parties.
- transmitting any other statement which is likely to create any liability (whether criminal or civil and whether for the employee or for the trust).
- downloading or disseminating material in breach of copyright.
- engaging in online chat rooms, instant messaging, social networking sites and online gambling.
- forwarding electronic chain letters and other materials.
- accessing, downloading, storing, transmitting or running any material that presents or could present a risk of harm to a child.

Any such action will be treated very seriously and may result in disciplinary action up to and including summary dismissal.

Where evidence of misuse is found, the trust may undertake a more detailed investigation in accordance with our Disciplinary Policy, involving the examination and disclosure of monitoring records to those nominated to undertake the investigation and any witnesses or members of management involved in the disciplinary procedure.

If necessary, such information may be handed to the police in connection with a criminal investigation.

Digital Cameras

The trust encourages the use of digital cameras and video equipment. However, staff should be aware of the following guidelines:

- Publication of photos should be consistent with Trust guidelines, including receipt of appropriate consent and guidelines for use of social media and for publicity purposes, as set out in the social media section of this policy.
- The use of personal digital cameras in school is not permitted, including those which are integrated into mobile phones, iPads or similar.
- All photos should be downloaded to the trust network as soon as possible.
- The use of mobile phones for taking photos of pupils is not permitted.

File Storage

Staff members have their own personal area on the network, as well as access to shared network drives. Any trust related work should be stored on one of these network drives. Personal files are not permitted on the network areas. Staff are responsible for ensuring they have rights for the storage of any file in their area for example, copyright music files.

Use of removable media should be avoided wherever possible. Any files stored on removable media must be stored in accordance with the Cyber Security Policy, summarised as follows:

- If information/data is to be transferred, it must be saved on an encrypted, password protected, storage device.
- No trust data is to be stored on a home computer or un-encrypted storage device.
- No confidential or trust data which is subject to the Data Protection Act should be transferred off site unless it is sent by secure email.
- The information should be deleted from the removable media as soon as the intended purpose has been served.
- Removable media should not be used for permanent storage of data – SharePoint and OneDrive are available to all staff and are more secure and appropriate locations for longer term storage of information.

Use of Own Devices

Wherever possible and provided, staff should always use Trust-provided devices for all work activities. However, staff can use their own devices at work and outside of work for work related activities provided the terms of this policy are met in situations where use of a work device is not possible. The trust reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the trust's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms. This policy is not designed to offer protection for the device itself. The safety of the user's own device is the responsibility of the user.

Mobile devices within the context of this policy includes any mobile phone, tablet, laptop, MP3/iPod or other device which can connect with the internet or mobile networks or taking image or sound recordings.

The trust embraces the use of new and mobile technologies and acknowledge they are a valuable resource in the classroom having educational purpose.

However, by accessing the trust's systems and networks, it is likely that staff will use personal data and so must abide by the terms of the Data Protection Act 2018 when doing so (including ensuring adequate security of that personal information).

All employees must agree to the following terms and conditions to be able to connect their devices to the trust network:

- All staff who wish to use their own devices to access the trust's network must sign and return the statement at the conclusion of this policy.
- When in School, staff should connect their device via the trust's wireless network for security.
- When out of School, staff should access work systems on their mobile device using SharePoint.
- All internet access via the network is logged and as set out in the Acceptable Use policy, employees are blocked from accessing certain websites whilst connected to the TDET network.
- The use of camera, microphone and/or video capabilities are prohibited whilst in School unless this has been approved by the principal. If approved, any pictures, videos or sound recordings can only be used for School purposes and cannot be posted or uploaded to any website or system outside of the trust network.
- You must not use your device to take pictures/video/recordings of other individuals without their advance written permission to do so.
- Any apps or software which are downloaded onto the user's device whilst using the trust's own network is done at the user's risk and not with the approval of the school.
- Devices may not be used at any time to:
    - Store or transmit illicit materials.
    - Store or transmit proprietary information belonging to the trust.
    - Harass others.

    - Act in any way against any section of this policy and other safeguarding and data related policies.

- Technical support is not provided by the trust on the user's own devices.
- To prevent unauthorised access, devices must be password/pin/fingerprint protected using the features of the device and a strong password is required to access the trust network. The owner of the device is responsible for ensuring that the device has appropriate anti-virus, firewall, and other protection to prevent cyber-attack.
- When using personal data, it is the user's responsibility to ensure they keep data secure on their device. This includes preventing theft and loss of data (for example, through password protection and cloud back up), keeping information confidential (for example, by ensuring access to emails or sensitive information is password protected) and maintaining that information.
- The trust does not accept responsibility for any loss or damage to the user's device when used on the trust's premises. It is up to the user to ensure they have their own protection on their own device (such as insurance).
- Staff are not permitted to install email apps which allow direct access to School/Trust emails without use of a login/password.
- If information is particularly sensitive, then users should ensure that the data is either appropriately secured or deleted from the device (including from any local copies which may have been stored on the device.
- In the event of any loss or theft of personal data, this must be reported immediately as a data breach in accordance with the trust's Data Breach Policy.
- The trust may require access to a device when investigating policy breaches (for example, to investigate cyber bullying).
- Staff are not permitted to share access details to the trust network or Wi-Fi password with anyone else.
- The trust will not monitor the content of the user's own device but will monitor any traffic over the trust system to prevent threats to the trust's network.
- The trust reserves the right to disconnect devices or disable services without trust.
- The employee is expected to always use his or her devices in an ethical manner and adhere to the trust's policy as outlined above.
- The employee is personally liable for all costs associated with his or her device.
- The trust reserves the right to take appropriate disciplinary action up to and including summary dismissal for non-compliance with this policy.

Landline Phones

The Trust phone systems are available to use by any department to communicate with suppliers, parents, authorities and other staff members.

- All phone contact with parents regarding school issues will be through the trust's phones. Personal phone numbers should not be given to parents at the school.
- Trust Phones are not to be used for personal matters.
- The trust records in-coming phone calls to:
    - Review and improve services
    - Monitor and review quality of care
    - Train, develop and manage staff.
    - Prevent, detect, investigate and prosecute allegations, complaints, claims and / or fraud relating to Trust staff, parents and pupils
    - Protect staff and pupils

Mobile Phones

Mobile phones are permitted in the trust with the following restrictions:

- They are not to be used when members of staff are directly supervising or working with children. Whilst members of staff are working in the classroom they should be securely stored in a bag/cupboard/locker.
- Personal mobile phone cameras are not to be used on school trips. The trust provides digital cameras for this purpose.
- All phone contact with parents regarding school issues will be through the trust's phones. Personal mobile numbers should not be given to parents at the school.
- Trust Phones are not to be used for personal matters.
- The trust can record in-coming and out-going phone conversations.
- If you record calls, callers must be made aware that the conversation is being recorded and the reasons for doing so. Your trust's phone system probably has an automated option you can use/ adapt.
- All non-standard recordings of phone conversations must be pre-approved, and consent obtained from all parties involved.

Use of WhatsApp

WhatsApp is permitted for use on trust issued devices or personal devices for trust business provided that no sensitive data is shared.

Reference should also be made to the Social Media section of this policy.

Monitoring of the ICT Systems

The trust may exercise its right to monitor the use of its ICT systems. This includes websites accessed, the interception of e-mail and the viewing of data stored, where it believes unauthorised use of the trust's ICT system is or may be taking place or the system is or may be being used for criminal purposes. Any inappropriate material found will be deleted. Monitoring software is installed to ensure that use of the network is regularly checked by IT Technical Services to ensure there are no pastoral or behaviour concerns or issues of a safeguarding or prevent nature.

Other reasons for monitoring the ICT systems include the need to:

- ensure operational effectiveness of the services provided.
- maintain the systems.
- prevent a breach of the law, this policy or any other trust policy.
- investigate a suspected breach of the law, this policy or any other trust policy.

Any unauthorised use of the trust's ICT systems, cloud-based ICT systems, the internet, e-mail and/or social networking site accounts which the Trust IT Lead considers may amount to a criminal offence or is unlawful shall, without notice to the user concerned, be reported to the police or other relevant authority. The trust reserves the right to audit and/or suspend a user's network, e-mail and/or application account(s) pending an enquiry, without notice to the user concerned.

Remote working

This section applies to individuals who work from home and/or use or access trust systems or information from home or while working remotely. It applies to information in all formats, including paper records and electronic data.

Remote working means working off the trust site. This includes working while connected to the trust networks.

A mobile device is defined as a portable device which can be used to store or process information. Examples include but are not limited to laptops, tablets, USB sticks, removable disc drives and smartphones.

Working from home presents both significant risks and benefits.

Staff may have remote access to information held on secure trust servers but without the physical protections available in the trust. Without the network protections provided by firewalls and access controls, there are much greater risks of unauthorised access to data as well as a risk of loss or destruction of data. There are also greater risks posed by information "in transit" (i.e., moving data between office and home).

The risks posed by working from home can be summarised under three headings:

- *Reputational*: the loss of trust or damage to the trust's relationship with its community.
- *Personal*: unauthorised loss of or access to data could expose staff or students to identity theft, fraud or significant distress; and
- *Monetary*: regulators such as the ICO can impose financial penalties and those damaged because of a data breach may seek redress through the courts.

The decision as to whether to allow partial or full-time homeworking in relation to any given role rests with management.

Any member of staff working from home is responsible for ensuring that they work securely and protect both information and trust-owned equipment from loss, damage or unauthorised access.

Managers are responsible for supporting staff adherence with this policy. Additional measures may be put in place by management to ensure the rules contained within this policy are adhered to (for example, monitoring or supervision).

Key Principles of Homeworking

Staff working from home must ensure that they work in a secure and authorised manner. This can be done by complying with the principles below: -

- To adhere to the principles of the Data Protection Act 2018 and the trust's Data Protection Policy in the same way as they would if they were working on site.
- Access to personal data must be controlled. This can be done through physical controls, such as locking the home office for physical data and locking the computer by using strong passwords (a mixture of letters, numbers and special characters).
- No other members of the household should know or be able to guess your work-related password(s). Passwords should not be written down or left on display for others to see.
- Automatic locks should be installed on IT equipment used to process trust information that will activate after a period of inactivity (i.e., computers should automatically lock requiring you to sign back in after this period).
- IT equipment used to process and store trust information in the home must be kept in a secure place where it cannot be easily accessed or stolen.
- Portable mobile devices used to process and store trust information should be encrypted where possible (or at least password/pin code protected) and should never be left unattended in a public place.
- IT equipment in the home used to process trust information should not be used where it can be overseen by unauthorised persons.
- It is the responsibility of each member of staff to ensure that they are working in a safe environment at home. No health and safety risks must be taken when using this equipment.
- Access to certain systems and services by those working from home or remotely may be deliberately restricted or may require additional authentication methods (such as two factor authentication which requires an additional device to verify individuals). Any attempt to bypass these restrictions may lead to disciplinary action.
- All personal information and in particular sensitive personal information should be encrypted/password protected before being sent by email where possible. Extra care must be taken when sending emails where auto-complete features are enabled (as this can lead to sending emails to similar/incorrect email addresses). The rules relating the sending of emails are outlined in the 'Trust Email' section of this policy.
- Staff should always use trust email addresses when contacting colleagues or students. If telephoning a child or parent at their home, staff should ensure that their caller ID is blocked.
- Any technical problems (including but not limited to, hardware failures and software errors) which may occur on the systems must be reported to the IT Services team immediately.

- To adhere to the trust's Data Retention Policy and ensure that information held remotely is managed according to the data retention schedule. Data should be securely deleted and destroyed once it is no longer needed.
- If communicating remotely via video conferencing and social media, staff must adhere to using only those platforms which have been approved by the trust and follow the trust's guidance on the safe use of video conferencing.
- To be vigilant to phishing emails and unsafe links. If clicked these links could lead to malware infection, loss of data or identity theft.
- Staff should not access inappropriate websites on trust devices or whilst accessing trust networks.
- Staff who have been provided with trust-owned IT equipment to work from home must:
    - only use the equipment for legitimate work purposes.
    - only install software on the equipment if authorised by the trust IT support. Please note that this includes screen savers, photos, video clips, games, music files and opening any documents or communications from unknown origins.
    - ensure that the equipment is well cared for and secure.
    - not allow non-staff members (including family, flatmates and friends) to use the equipment or to share log in passwords or access credentials with them.
    - not attempt to plug in memory sticks into the equipment unless encrypted and supplied by the trust).
    - not collect or distribute illegal material via the internet.
    - ensure anti-virus software is regularly updated; and
    - to return the equipment securely at the end of the remote working arrangement.
- Staff who process trust data on their own equipment are responsible for the security of the data and the devices generally as set out in the 'Use of Own Equipment' section of this policy.
- Staff are responsible for ensuring the security of trust property and all information, files, documents, data etc within their possession, including both paper and electronic material. Physical data (i.e., paper documents, which includes documents printed at home) must be secured and staff must ensure that:
    - Paper documents are not removed from the trust without the prior permission of their line manager. When such permission is given, reasonable steps must be taken to ensure the confidentiality of the information is maintained during transit. The information is not to be transported in see-through bags or other un-secured storage containers.

- Paper documents should not be used in public places and not left unattended in any place where it is at risk (e.g., in car boots, in a luggage rack on public transport).
- Paper documents taken home or printed at home containing personal information, sensitive data and confidential information are not left around where they can be seen, accessed or removed.
- Paper documents are collected from printers as soon as they are produced and not left where they can be casually read.
- The master copy of the data is not to be removed from trust premises.
- Paper documents containing personal data are locked away in suitable facilities such as secure filing cabinets in the home just as they would be in the trust.
- Documents containing confidential personal information are not pinned to noticeboards where other members of the household may be able to view them; and
- Paper documents are disposed of securely by shredding and should not be disposed of with the ordinary waste unless it has been shredded first.

- Any staff member provided with trust devices must not do, cause or permit any act or omission which will avoid coverage under the trust's insurance policy. If in any doubt as to whether acts or omissions will have this effect, the staff member should consult their line manager immediately.
- All staff must report any loss or suspected loss, or any unauthorised disclosure or suspected unauthorised disclosure, of any trust-owned IT equipment or data immediately to the Trust IT Lead in order that appropriate steps may be taken quickly to protect trust data. Failure to do so immediately may seriously compromise trust security. Any breach which is either known or suspected to involve personal data, or sensitive personal data shall be reported to the Data Protection Officer (full details of the officer can be found in our Data Protection Policy).

Social media

For the purposes of this policy, the Trust defines social media as 'any websites and applications that enable users to create and share content or to participate in social networking'. Social networking sites and tools include, but are not limited to, Facebook, X (Twitter), Snapchat, TikTok, LinkedIn, Myspace, Flickr, YouTube and Instagram. It also includes forums and discussion boards such as Yahoo! Groups or Google Groups, online encyclopaedias such as Wikipedia, and any other web sites which allow individual users or organisations to use simple publishing tools.

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the

misuse/abuse of these facilities can range from inappropriate to criminal and the Trust has this policy in place to deal with any misuse of social media.

The widespread availability and use of social media applications bring opportunities to understand, engage, and communicate in new, relevant and exciting ways. It is important that we can use these technologies and services effectively and flexibly. However, it is also important to ensure that we balance this with duties to the Trust, the community, our legal responsibilities and our reputation.

Through appropriate use of social media, we aim to:

- Safeguard all pupils and promote wellbeing.
- Ensure users are not exposed to risk because of their actions.
- Use social media in a respectful, positive and productive way which respects all parties involved.
- Ensure that the reputation of the Trust, its staff, committee members and trustees is protected and that stakeholders understand their ambassadorial role regarding the Trust.
- Protect the Trust from legal risks.
- Ensure that any users are able clearly to distinguish where information provided via social media is legitimately representative of the Trust.

In the event of unsafe and/or unacceptable behaviour, disciplinary or legal action (including gross misconduct leading to dismissal) will be taken, if necessary, to support safer working practice and minimise the risk of malicious allegations against staff and others who have contact with learners.

Curriculum use

There are many legitimate uses of social media within the curriculum, and to support student learning and to share news with the wider Trust community. For example, the Trust, academies and sub-departments of the academies have official Twitter, Instagram, X, Tik Tok and Facebook accounts.

There are also many possibilities for using social media to enhance and develop pupils' learning and to keep the Trust Community and our supporters in touch with the Trust.

Trust/Academy social media accounts

When using Trust/academy social media accounts and/or social media accounts using the name of Thomas Deacon Education Trust, a Trust or academy logo, or clearly attached to the Trust in some way, the following practices must be observed:

- Any account should be entirely separate from any personal social media accounts held and should be linked to an official Trust/academy email account.

- The social media account must be approved by the appropriate Executive Group member/Principal.
- The content of any Trust-sanctioned social media site and/or social media accounts using the name of Thomas Deacon Education Trust or associated academy, a Trust/academy logo, or clearly attached to the Trust in some way, should be entirely professional and should reflect well on the Trust.
- Staff must not publish photographs of pupils without appropriate consent. For pupils under the age of 13, written consent must be obtained from parents/carers. For pupils aged 13 and over, who are deemed to have the capacity to understand, consent should be obtained directly from the pupil. This pupil consent overrides any previous parental consent. When publishing images, only the pupil's first name and initial of surname should be used, unless specific permission has been given for the full name to be used. In cases where there are safeguarding concerns, no identifying information should be published with the photograph. Staff should always verify the most current consent status before publishing any images. The school will maintain an up-to-date record of consent preferences for all pupils.
- Any links to external sites from the accounts must be appropriate and safe; if they are shared these must be reputable sites. Only appropriate hashtags should ever be used.
- Any inappropriate comments on, or abuse of, Trust/academy-sanctioned social media and/or social media accounts using the name of Thomas Deacon Education Trust/Academy, a Trust/academy logo, or clearly attached to the Trust in some way, should immediately be removed. It is the responsibility of everyone using the site and social media in general to report abuse immediately.

The Trust has official Facebook, X and Linked in pages, managed by staff identified at Trust level. Our academies all have official social media pages, including Facebook, X, Instagram and Linked In, which are managed by staff identified at Trust level. Staff members who have not been authorised to manage, or post to, the account, must not access, or attempt to access these accounts.

Some of our academies have departmental social media pages, including X, Instagram and Tik Tok, which are managed by staff at academy level.

The Trust has guidelines for what can and cannot be posted on its social media accounts. Those who are authorised to manage the account must ensure they always abide by these guidelines.

Communication with students via social media

Staff must not have 1:1 communication, including direct messaging (DM), with pupils through any social media, apart from via school email accounts, Google Meet hangouts via a Trust/academy account and Trust/academy mobile devices for text messaging.

Staff should not request or accept any current student of the Trust of any age or any ex- student of the Trust under the age of 18 as a friend, follower, subscriber or similar on any personal social media account unless they are the parent of the pupil or a close family member.

It is advisable that staff do not have contact with past pupils (above school age). Staff may remain in communication with past pupils via a Trust/academy email account or the Trust/academy social media accounts.

Any communication received from current pupils on any personal social media sites must be reported immediately to the DSL. If any member of staff is aware of any inappropriate communications involving any student in any social media, these must immediately be reported to the DSLs.

Members of staff must ensure that, wherever possible, and where the social media site allows, their privacy settings on social media sites are set so that pupils cannot access information relating to their personal lives or follow them on their personal accounts.

All email communication between staff and pupils of the Trust on school business must be made from an official Trust/academy email account (any deviation from this in an emergency must at once be reported to the line manager). Staff should not use personal email accounts or personal mobile phones to contact pupils of the Trust/academy, nor should any such contact be accepted, except in circumstances such as school trips or away matches that have been given prior approval.

Staff use of social media

We encourage staff to positively promote the Trust and our academies on professional networking sites such as LinkedIn. However, staff should exercise discretion and good judgement when posting about their work. Avoid sharing confidential information, discussing specific pupils or parents, or making negative comments about colleagues or the Trust. Instead, focus on sharing achievements, highlighting events, and showcasing the Trust's positive impact. If you're unsure about what is appropriate to post, consult your line manager or the Communications Team for guidance.

Staff must not post images on any unofficial Trust/academy social media account that includes pupils, unless sharing posts made from a Trust/academy official social media account.

Staff are instructed to consider the reputation of the Trust in any posts or comments related to the Trust/academy on any social media accounts. Reputational breaches by staff are dealt with via the TDET Disciplinary Policy.

Staff must be mindful of their role as ambassadors of the Trust, and that any inappropriate or offensive content published on a private social media account may cause reputational damage for the Trust and so can be considered a disciplinary matter in line with the Disciplinary Procedure.

Members of staff are responsible for overseeing and monitoring any social media account attributed to their area of responsibility where the social media account is using the name of Thomas Deacon Education Trust, a Trust/academy logo, or clearly attached to the Trust in some way.

Safeguarding

Those working with children have a duty of care and a statutory duty to report signs of potential radicalisation (the Prevent duty) but also need to be on the lookout for cyber bullying and other activities on social media which might affect the mental health of learners.

Staff will receive regular training on safeguarding matters, including online safety.

General behaviour

Staff are expected to adopt high standards of behaviour to retain the confidence and respect of colleagues and learners both within and outside of academy. They should maintain appropriate boundaries and manage personal information effectively so that it cannot be misused by third parties e.g. for 'cyber-bullying' or identity theft.

When using social media staff and others should:

- Never share work login details or passwords.
- Keep personal phone numbers private.
- Never give personal email addresses to learners or parents.
- Staff should use privacy settings on their personal social media accounts to limit who can see their posts and personal information. Not make 'friends' of learners at the Trust/academy because this could potentially be construed as 'grooming', nor should they accept invitations to become a 'friend' of any learners.
- Carefully consider contact with a learner's family members because this may give rise to concerns over objectivity and/or impartiality.
- Keep any communications with learners transparent and professional and should only use the Trust's/academies' systems for communications. (If there is any doubt about whether communication between a learner/parent and member of staff is acceptable and appropriate a member of the Senior Leadership Team should be informed so that they can decide how to deal with the situation).

Before joining the Trust, new employees should check any information they have posted on social media sites and remove any post that could cause embarrassment or offence.

Misuse of social media

While acknowledging the benefits of social media and the internet it is also important to recognise that risk to the safety and well-being of users is ever-changing and that the misuse/abuse of these facilities can range from inappropriate to criminal. Misuse can be summarised as follows:

Contact

- Commercial (tracking, harvesting personal information).
- Aggressive (being bullied, harassed or stalked).
- Sexual (meeting strangers, being groomed).
- Values (self-harm, unwelcome persuasions).

Conduct

- Commercial (illegal downloading, hacking, gambling, financial scams).
- Aggressive (bullying or harassing another).
- Sexual (creating and uploading inappropriate material).
- Values (providing misleading info or advice).

Content

- Commercial (adverts, spam, sponsorship, personal information).
- Aggressive (violent/hateful content).
- Sexual (pornographic or unwelcome sexual content).
- Values (bias, racism, misleading info or advice).

Serious misuse of social media

Learners, staff and volunteers must be aware of what is 'criminal' when using social media or the internet and electronic communication in general.

While the list below is not exhaustive, it provides some guidance in assessing the seriousness of incidents as well as determining appropriate actions.

All incident types below are considered criminal in nature, but incidents would be subject to a full investigation to determine whether a crime has been committed or not.

- Copyright infringement through copying diagrams, texts and photos without acknowledging the source.
- Misuse of logins (using someone else's login).
- Distributing, printing or viewing information on the following:
    - Soft-core pornography.
    - Hate material.
    - Drugs.
    - Weapons.
    - Violence.
    - Racism.
- Distributing viruses.
- Hacking sites.
- Gambling.
- Accessing age restricted material.
- Bullying of anyone.
- Viewing, production, distribution and possession of indecent images of children.

- Grooming and harassment of a child or young person.
- Viewing, production, distribution and possession of extreme pornographic images.
- Buying or selling stolen goods.
- Inciting religious hatred and acts of terrorism.
- Downloading multimedia (music and films) that has copyright attached. (Although this is illegal most police forces would treat this as a lower priority than the cases above).

The Trust's policies and protocols on child protection, safeguarding and e-safety must be followed if any apparent, suspected or actual misuse appears to involve illegal or inappropriate activity:

- Child sexual abuse images.
- Adult material which potentially breaches the Obscene Publications Act.
- Criminally racist material.
- Other criminal conduct, activity or materials.
- Potential radicalisation or extremism.

Any actions online that impact on the Trust and can potentially lower the Trust's (or someone in the Trust's) reputation in some way or are deemed as being inappropriate will always be responded to.

If any member of staff, learner or parent/carer is found to be posting libelous or inflammatory comments on social networking sites, this will be addressed by the Trust in the first instance. If appropriate, disciplinary action will result. However, where necessary, the police will be involved and/or legal action pursued.

Handling negative comments

When representing the Trust or a TDET academy, it is important to address offensive comments promptly and with sensitivity. If a conversation takes a negative turn, users should act by blocking, reporting, or deleting other users or their comments / posts. Actions should be taken based on the severity and nature of the situation:

- Block: Use this when a user repeatedly engages in harassing, abusive, or inappropriate behaviour towards the Trust or school. Blocking is appropriate when direct communication with the user is persistent, unwanted and potentially harmful. The blocking of an account is to be agreed by a member of the Executive Group for central team social media accounts or the principal for academy social media accounts.
- Report: Content or behaviour that violates the platform's community guidelines or terms of service is to be reported. This might include instances of harassment, hate, speech, threats, bullying, or other forms of misconduct. Reporting helps to ensure that the platform administrators can review and take appropriate action.

- Delete: Comments, posts, or other content that is offensive, inappropriate, or violates our rules is to be deleted. Deleting comments is suitable when content is against our standards.
- Hide: Use the hide function to moderate comments or posts that may not necessarily violate community guidelines but are still inappropriate or off topic. This can be useful when managing discussions or preventing spam.

If anyone experiences or witnesses abuse from colleagues on social networking sites, they must follow the established central team / academy protocols for reporting such incidents.

In the event of complaints directed at the school through comments on its social media profiles, the social media lead for that platform should respond politely and suggest moving the discussion offline to follow the Trust's Complaints Policy. For example: 'Thank you for bringing this to our attention. Please email [EMAIL ADDRESS] so we can address this matter'.

Acceptable Use Agreement

To be completed by all staff

As a trust user of the network resources/equipment I hereby confirm that I have read and understood the Acceptable Use Policy and that I agree to follow the trust's rules (set out within the Acceptable Use Policy) on its use. I will use the network/equipment in a responsible way and observe all the restrictions explained in the trust's Acceptable Use Policy. If I am in any doubt, I will consult the Trust IT Lead.

I agree to report any misuse of the network to the Trust IT Lead. Moreover, I agree to report any websites that are available on the trust's internet that contain inappropriate material to the TDET Safeguarding Lead and IT Services. Finally, I agree to ensure that portable equipment such as cameras, iPads or laptops will be kept secured when not in use and to report any lapses in physical security to the Trust IT Lead.

Specifically, when using trust devices:

- I must not use these devices for inappropriate purposes.
- I must only access those services for which permission has been granted.
- I will not download, use or upload any material which is unsuitable within a school setting or that may cause disruption to the trust's network.

If I do not comply with the rules, I understand that this may result in loss of access to these resources as well as other disciplinary action. I realise that staff under reasonable suspicion of misuse in terms of time or content may be placed under retrospective investigation or have their usage monitored.

I understand that the trust will monitor communications to uphold this policy and to maintain the trust's network (as set out within this policy).

Signed ……. Date ……

Print name ……