Durrington Multi Academy Trust
Information Communication Technology (ICT)
Acceptable Use Policy (inclusive of social media)

Introduction

Information Communication Technology (ICT) is provided to support and improve the teaching, learning and wellbeing in trust schools as well as ensuring the smooth operation of the wider administrative and financial systems the trust needs to run effectively.

This policy sets out the trust's expectations in relation to the appropriate use of ICT by all users who are part of the trust. This includes hardware, software, networks and social media, whether these are owned/provided by the trust, personally owned/operated and/or used on a trust network(s).

In addition the policy details the expectations of employees regarding the safe use of ICT and (if employees use it) social media. The acceptable use of ICT will be covered during the induction process for employees. The policy, for reference, will remain open to access by trust employees stored centrally on the network. Ongoing training, support and advice will be provided by the trust as well as updates to this policy as/when deemed necessary. Training can/will also be provided at the specific request of an individual/group of staff. We encourage all users to be proactive in asking for advice and support so as not to place themselves or the trust at risk.

This policy forms part of the terms and conditions of all employee's contract of employment and may be amended at any time, however a breach of this policy is likely to result in disciplinary action and referral to external agencies in the event of illegal activity.

Scope and purpose

The purpose of this policy is to ensure that employees are clear on the trust's rules and personal obligations of employees when using ICT and to protect individuals and wider schools/organisations that are part of the trust from risk. In addition, it provides clear guidance to employees if/when they are using social media to reduce risks to them as individuals and the trust as their employer.

Key definitions

Employees: these are all adults who have a contract (casual, fixed term or permanent) of employment with DMAT.

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

Users: encompassing employees this is a broader group of individuals some of whom may have no direct contract of employment but may have reason to visit a trust site and/or use the trust provided ICT facilities as part of their visit. "Users" include groups* such as

- Trustees & governors
- Trainee teachers & volunteers
- Casual supply staff
- Adults make one off or periodic visits to a trust school(s) for training and/or monitoring purposes
- Contractors, consultants and any other third parties employed cleaning and catering staff.

ICT includes* all trust/school commissioned and maintained:

- Electronic hardware and networks
- Cloud services inc data on and off site
- Software & applications
- Communication systems including, but not limited to
    - email
    - telephone
    - mobile devices & handheld radios
- Remote access

ICT Support provider: this includes the central DMAT ICT Services Team, onsite technician or contracted ICT support provider.

Ensuring ICT is used in an appropriate way is the responsibility of every user; this also applies to trust equipment and for employees only their personal use of social media which may be on or off trust/school environments.

Policy breaches

Employees may be required to act if it is deemed that they have breached this policy (examples being removing internet postings or images). Failure to comply with such a request may result in disciplinary action which would be managed through the disciplinary procedure.

Users, if in breach of this policy, may be barred from use of trust ICT facilities. If employees are found in serious breach of this policy the trust may consider this to be gross misconduct which could lead to dismissal, legal action or, in the case where a user has potentially broken the law, police involvement. If deemed necessary a user may be required to share relevant password and login details.

If you reasonably believe that any adult user has breached this policy, you should report it without delay to the Headteacher^ of your school or CEO of the trust.

Trust personnel responsible for implementing the policy

The local governing body of each school has overall responsibility for the effective operation of this policy, however day-to-day responsibility for its operation is delegated to the Headteacher^ / Senior Leadership team on each school site.

Responsibility for monitoring and reviewing the operation of this policy and making recommendations for

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

change to minimize risks also lies with each school's Headteacher^, the CEO of the trust, Director of IT and, if the school has one, the designated member of the SLT responsible for ICT.

All employees have a responsibility to operate within the boundaries of this policy, ensuring that they understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements. Employees should ensure that they take the time to read and understand it. If further clarification is required users should be preemptive in speaking to a member of senior staff within the school/trust or the Director of ICT Services before acting.

Any misuse of ICT should be reported to the Headteacher^ or Director of IT immediately.

Monitoring of the policy

The physical hardware, all electronically stored materials, information that has been printed and licensed software installed on all trust ICT systems remain the property of the trust. As such users of trust ICT should have no expectation of privacy when using trust devices (on or offsite) or when communicating via trust networks/software.

The trust reserves the right to monitor, intercept and review, without notice, staff activities using our ICT hardware, software and/or networks (including but not limited to social media postings and activities), to ensure that trust policies are being complied with and for legitimate business purposes. Users consent to such monitoring by using trust hardware/software and/or networks.

Monitoring might include, without limitation, the tracking, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other uses of the systems, as well as keystroke capturing and other network monitoring technologies.

We may store copies of such data or communications for a period of time after they are created, and may delete such copies from time to time without notice.

Employees must not use any trust device, network, hardware or software for any matter that you wish to be kept private or confidential from the trust. Employees are also reminded that any/all communication using trust devices, networks and software may need to be disclosed to third parties (e.g. under GDPR) and that all communication, at all times, needs to remain professional

Any breach of this policy may result in disciplinary action and the trust reserves the right to involve wider agencies (such as the police) if there is the possibility that illegal activity has occurred.

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

Appendices

Several appendices are included that also form part of the policy. These are structured to give topic specific advice and guidance to users.

Appendix A – Use of the internet

Appendix B – Email communication & instant messaging

Appendix C – Use of mobile devices

Appendix D – Use of social media (network users and employees)

Appendix E – Private/personal use of trust ICT facilities

Appendix F – Use of mobile storage devices

Appendix H – Reporting concerns and statutory compliance

Appendix I - Student ICT usage agreement (secondary)

Appendix J - Associated documentation and policies

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

Appendix A: Use of the internet

Internet usage (general)

Employees are required to:

- Check your work emails at least twice a day (on work days). Email is used to communicate important messages to both staff and students regularly.
- Use their own, and only their own, login credentials (username and password) when accessing the network and all other software requiring passwords to access (e.g*. Outlook, Remote access, Arbor).
- Protect information (your own and that of others and the school) by not giving out personal information about a student, another employee or the school, to third parties unless you are sure (and you have permission to) that the request is valid. If in doubt speak to your local GDPR lead.
- Avoid visiting websites or downloading content that might be considered inappropriate/illegal or potentially harmful to the trust, students, other staff or the network. Examples of sites include*
    - Those with proxies
    - Dating sites
    - Hacking/hacking related sites
    - Sites containing or linking to pornographic content
    - Sites relating to non-educational gaming
    - Sites relating to gambling

  If an employee is in any doubt regarding the suitability of a website/content they should contact a member of the ICT team prior to downloading material/viewing content. DMAT takes additional steps to help protect all users, network hardware and software through using regularly updated firewalls and internet filtering services. Employees are reminded that viewing/downloading some material is illegal and the police or other authorities may be called to investigate such use. Internet history/use is stored on all devices connected to the trust's networks.

- Not publish or store copyrighted material on the school network or wider internet.
- Report any unsuitable/inappropriate/illegal content found on trust networks/hardware of software to the school's ICT support provider immediately
- Alert your schools ICT support provider and a member of the senior leadership team if you
    - receive any messages/attachments that make you feel uncomfortable or that you believe to be unsuitable/illegal.
    - view content that makes you feel uncomfortable or you think is unsuitable (even by mistake).

  Remember that everything you do on our trust network will be subject to monitoring
- Not, at any time (during or outside of work hours), use the Internet/network in a way that may interfere with the efficient running of the school (this includes storing excessive amounts of data-heavy files)

Employees using remote access services are required to use a device with appropriate permissions and security (for example a password protected computer and home network) in place before initiating this use (for guidance on what is required, speak to a member of your ICT support provider).

Employees are also advised not to give out personal information such as your address, telephone number

or mobile number over the internet without being sure that the receiver is from a reputable source.

User's, when opting to use trust ICT (e.g. using guest WiFi when on site) are required not to*

- use ICT in any way that could damage the network (physically or virtually)
- access, download or publishing any material that is illegal (users should be aware that by accessing the network their personal files and activity will be subject to monitoring)
- use the network in a way that has a negative impact on other users/employees (e.g. by downloading large files*)
- access any information that cannot be seen to directly relate to their reason for using the network/being on site (for example* not accessing student details unless there is a specific reason to do so).

If users have any questions about the use of trust ICT these should be referred to your schools ICT Support provider.

Failure to follow these expectations is likely to result in a user being banned from future use. Where there is the possibility that a user's behaviour has broken the law, the trust reserves the right to contact all necessary outside agencies (for example* the police).

Guidance specific to the use of the internet in the classroom/in front of students

This guidance must be followed every time you show electronic material to a class/group of students/student (for example Youtube clip).

- Prior to showing the material the employee must review, in full, the intended content and check that all the information intended to be shown is suitable for the audience it is being shown to.
- Employees are expected to check any material that could be considered "borderline" with your curriculum leader or member of SLT prior to showing it to the class.
- Employees must only show age appropriate material to the student(s). If material has no age rating then no clip will be shown that contains swearing, any form of racial, gender or other type of harassment/hate content, inappropriate sexual content, nudity, or anything that could reasonably be considered to cause offense to the watchers.

Appendix B: Email communication & instant messaging

Before sending an email/instant message, you should check it carefully and consider whether the content is appropriate, treating emails like you would any other form of formal written communication. When sending emails internally relating to a student(s) , staff should use the student's initials and form group/company in replacement of full names.

Although the email/instant messaging system is provided for business purposes we understand that employees may, on occasion, need to send or receive personal emails using their work email address. This should be kept to a minimum and should not affect or be to the detriment of you carrying out your role effectively. If sending personal emails from your work email account, you should show the same care in terms of content as when sending work-related emails.

Employees must never;

- Open an attachment on an unsolicited email from an unknown email address without first checking with your ICT support provider. Attachments could contain viruses or inappropriate/illegal content.
- Send personal data/information about any other stakeholder (e.g. student(s) and/or parent/carer) to any person(s) who are not employed by the trust other than;
    - Data that is necessary (e.g. safeguarding documentation, that requested by the police*)
    - Data which you have the express permission (e.g in the case of a student from the student themselves or from their parent/carer) to share with a named external professional

  All data/information sent externally in this way must be in encrypted format via Egress (or similar secure) system
- Use email/instant messaging to send or forward messages which are defamatory, obscene or could be considered in any way inappropriate. This will be considered under the disciplinary procedure.
- Use the school email/instant messaging system to make personal or offensive comments about students, employees, parents, carers or any other person(s) that could cause harm or offense
- Contact a student/students on their personal email addresses. Additionally, staff must ensure that all email communication is kept within appropriate hours (generally between 7.30am and 6pm on weekdays)
- Any communication to students must remain via their school email address, must only be in relation to school matters and must take place on weekdays. No communication should take place with any student after 6pm or at weekends.

If an employee receives an abusive, obscene, defamatory or any other form of concerning message or wider social media communication you should alert a member of the SLT. In the case of a message you suspect may contain malicious content e.g. viruses, unsolicited attachments or similar these should be forwarded to the ICT team investigation.

Trust advice is to use the “rule of 2” when communicating using email. This means employees seeking to speak to or meet with the other person (parent/carer/colleague/external professional) after two email communications have been exchanged (on the same topic/issue). Adopting this approach will reduce the potential for one or both parties misinterpreting information.

Personal email accounts
Users are advised not to use trust hardware/software of networks for the access/sending/receiving of personal emails. Logging into personal accounts/using trust networks/hardware/software makes the contents of personal email public and subject to monitoring.

Appendix C: Mobile Devices

The use of mobile tablets/laptops or other mobile or portable devices.

A variety of mobile devices are provided by the trust with the purpose of enhancing teaching & learning and making employee's work more efficient. These include*;

- Laptops and tablet computers and iPads
- Cameras (still and video)
- Mobile phones (principally used for safeguarding on trips)

As well as a range of other subject area/specific items.

The following expectations apply to all employees who use mobile devices provided by the Trust/school.

- Access to our wireless network must be approved by your school's ICT support provider.
- Employees must ensure that mobile devices that are on loan to them (from the school/trust) and have the facility to be password protected and are secured with a password/code. This is particularly important if you are taking the mobile device off site.
- Employees are expected to ensure that all trust owned devices in their care are securely locked away when they are not being used. You must not leave your mobile device in an unsafe place, for example in your car or unlocked classroom. Furthermore, devices are expected to be kept in the cases provided so as to reduce the risk of damage.
- Should an employee wish to take a trust/school owned mobile device off site it is the employee's responsibility (in advance of doing this) to:

    a) Gain permission from a member of SLT or Director of ICT Services and sign a request to take ICT offsite form as a record of receiving and taking responsibility for the device.
    b) Ensure they have appropriate insurance in place so as to cover damage or theft of the device when off site
    c) Ensure that when taken off site the device is sorted in a safe and secure way and that only the employee uses the device.
    d) Ensure the device remains password protected (where the device has the facility for this to be set up)

- In the event of a trust/school owned device being damaged a member or SLT or Director of ICT Services should be notified immediately.
- Employees are made aware that school/trust owned mobile devices are monitored (including historical use e.g. browser history). It is the employee's responsibility to ensure that only appropriate content (as set out in this policy) is sorted on the device. Failure to do so could result in a breach of this, or other, policies/laws (see appendix H)

The use of personal mobile devices on the network/in schools

- Personal mobile devices may be used on the trust's network(s) but are required (as compatible/applicable) to have up-to-date anti-virus installed before being connected to the network; it is the responsibility of the employee to get this checked by the school's ICT support provider.
- Personal mobile devices are not to be:

- used at any time in a classroom in front of a student(s)
- used to take pictures/record audio of any student(s).

The trust reserves the right to disable access to the wireless network for any user at any time.

Specific guidance on the recording (still images, video, sound clips) of students

It is acceptable to record images or video of students for legitimate school aims which could include:

- The displaying of excellent pieces of work
- Coaching (students and/or staff) for improved performance
- Publicity in advance or and after events
- In-school displays

However, the following rules apply to the staff recording the image/video:

- The member of staff must let any student/person being photographed or videoed know whether or not their image will be retained for further use,
- The member of staff must only use trust/school devices (never personal devices including personal storage devices such as memory sticks) to record images/video on.
- At no time must any images/video storage device (personal or trust owned) be taken to, or used in any location (on or off site) where students or other employees are changing clothing or could be in any state of undress (e.g. toilets. changing rooms, dressing rooms)
- The member of staff must, after recording the images, ensure they are moved and securely stored and be clear about the reason for their storage. Once the videos/images are no longer needed it is the member of staff who recorded the image's responsibility to delete these from the trust's network/devices.
- Personal data processed for any purpose should not be kept for longer than is necessary for that purpose. Staff must not take images of students without their knowledge or approval.
- The member of staff using the images/video is responsible for checking the permissions list (for both employees and students) before the use of the image/video.

Appendix D: Social media

It is recognized that social media (in all its forms) can be of use for both employees and students, both an educational and communication tool. However, employees' use of social media can pose a risk of others misunderstanding the intent behind online communications and/or the blurring of professional boundaries between children and young people and/or their parents or carers.

An employee could, if they were to use social media in an inappropriate way or with a lack of proper care could:

- share confidential information,
- cause damage to their own or another professionals' reputation
- cause reputational damage to the trust/individual school they work for, and/or
- jeopardize the trust's/school's compliance with its legal obligations.

These risks could also be the case during non-school hours.

The trust has the following guidelines which all employees are expected to follow in relation to their own use of social media. The guidelines apply whether social media is being used for business or personal reasons, whether during working hours or otherwise, regardless of whether the social media is accessed using trust ICT facilities or personally owned devices.

The following sections of the policy provide staff with guidelines and recommendations for using social media responsibly and safely and to protect trust employees.

Communication with individuals (principally but not exclusively students and parents/carers)

- Employees should exercise caution when using social media. Employees must block unwanted communications from students. In the (rare case) of offensive or harassing communications being sent to employees these should be sent to a member of SLT before the original user being blocked. Employees are personally responsible for what you communicate on social media.
- Employees should never knowingly communicate with a student/students (including ex-students up to the date of their 19th birthday) via social media* or via personal email accounts/personal mobile phones or similar. Any communication with students **must be** through the school network/a school device so this can be appropriately monitored. If there is a need to communicate directly with a student/students this should only be conducted through our usual channels e.g. school email address to school email address or by a phone call home. Staff should not use/communicate to the personal email addresses or mobile phone numbers of students.
- At no point should personal/private messages ever be sent to a student/students via social media by employees.

  (*the only exception to this is when general broadcast information is posted on school named/branded social media streams)
- Communication, if it is appropriate/necessary, should only ever be related to school business.

Specific guidelines in relation to employee's who run/operate social media streams for professional purposes. This includes school specific/branded social media streams* such as Twitter accounts & Youtube and as well aso social media streams that are personally operated (not branded/directly linked in name to the school/trust).

Employees who choose to set up/run such content streams are responsible for ensuring

- security of access to the account (s) is maintained
- the content posted is appropriate
- any commenting/sharing of content by third parties is managed carefully thus ensuring that the trust/school/colleagues or any other person(s) mentioned are not harmed.
- all necessary GDPR are followed

Specific guidelines in relation to employee's personal use of social media

- All employees should ensure that securing settings on their social media accounts are set to the highest level of privacy. This is to protect you. (The DMAT ICT Services team are available and willing to offer advice and support as necessary to employees)
- If you decide to disclose your affiliation with DMAT/your school, you must also state that your views do not represent those of your employer. For example, you could state, "views/comments/postings are personal and in no way representative of the views of my employer". You should also ensure that your profile and any content you post are consistent with the professional image you present to students and colleagues.
- Employees should avoid social media communications that might be misconstrued in a way; for example social media postings that could damage your own professional integrity and those that

could damage school/trust reputation, even indirectly.

- Employees should make it clear in social media postings that they are speaking on their own behalf e.g. writing in the first person and use a personal email address when communicating via social media.
- Employees are responsible for what they communicate on social media. Remember that what you publish might be available to be read by the masses (including the school itself, future employers and social acquaintances) for a long time. Keep this in mind before you post content.
- Employees should avoid posting comments about sensitive school related topics; an example could be the school's/trust's stance in relation to a specific issue or school performance. Even if you make it clear that your views on such topics do not represent those of your school/the trust, your comments could still damage your own (or the Trust's) reputation and/or be upsetting to colleagues or students.
- If you are uncertain or concerned about the appropriateness of any statement or posting, refrain from making the communication until you discuss it with a member of site SLT.
- If you see content in social media that disparages or reflects poorly on the school/trust or one of our stakeholders, you should print out or screenshot the content and then give this/report this to the Headteacher^/CEO as soon as possible.

In addition to this, employees should not post or share anything/including any viewpoints (personal to them or not) that could bring the trust, trust leaders/governors/trustees and/or employees into disrepute or damage the wider reputation of the trust or its schools.

Employees should be aware that breaching the above guidelines may lead to disciplinary action being taken.

Appendix E: Personal use of ICT systems, services and facilities

- The trust does allow for limited personal use of the ICT facilities. It is expected that personal use, wherever possible, is limited to non-working time e.g. at lunchtime, before/after normal working hours. Examples of limited use would be responding briefly to an incoming personal e-mail or telephone call or to deal with a non-work-related emergency.
- An employee spending significant amounts of time making personal use of the internet, e-mail, communication equipment* is not acceptable.
- The following guidance must be adhered to if an employee chooses to make personal use of trust ICT systems/services and facilities.

The use of trust ICT must not:

- interfere with your (or others') work; examples include*
    - it is not acceptable for an employee to use the internet or network software in a way that triggers multiple securus breach reports)
    - classroom based staff using ICT for personal purposes during lesson contact time or at any other time they are responsible for the supervision of students.
- involve more than minimal amounts of working time;
- incur any significant expense to the trust and/or tie up a significant amount of resources (virtual or physical)
- involve storage of any personal information or files on any part of the ICT network.
- involve the downloading or storage of any copyrighted material or material that is illegal
- Involve the viewing of any material deemed inappropriate in a professional context
- Involve the downloading or installing of any personal software onto the network or trust devices
- lead to personal gain (financial or otherwise) for the member of staff.

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

Before undertaking personal use, employees should ask themselves the following questions.

- Would the actions be considered unacceptable if viewed by a member of the public?
- Would managers, auditors or others in similar positions call into question the cost effectiveness of use of work time or use of school/trust ICT networks/devices?
- Will personal use have a negative impact upon the work of colleagues (e.g. in terms of their motivation and morale)?
- Could personal use bring the trust/schools directly or indirectly into disrepute?

Personal use should not be undertaken if the answer to any of these questions is yes. The responsibility for ensuring that any personal use is acceptable rests with the individual. Employees should seek guidance from their line manager if they have any doubts concerning the acceptability of their personal use. If any doubt remains, then that form of personal use should not be undertaken.

Employees should be aware that breaching the above guidelines may lead to disciplinary action being taken.

Appendix F - Use of mobile storage devices.

Mobile storage devices are defined as any piece of hardware that can store electronic material (files/media/video/images etc) and can be easily moved between devices in a “plug and play” type way. (Examples* include USB sticks and external hard drives)

The trust/schools provide a range of remote access facilities, cloud storage and software and portable devices that are all password protected to support employees in their work. These services/hardware are provided to reduce the need for staff to save/transfer information onto/off mobile storage devices.

It is however recognised that some employees wish to use mobile storage devices. If an employee makes the choice to use a mobile storage device the following guidelines must be followed;

- All storage devices must be password protected and/or encrypted
- Storage devices should be regularly virus checked so ensure that no malicious material is transferred onto the trust’s network.
- Work related material on the storage device should be regularly backed up on the system to minimize the risk of loss.
- Storage devices should uniquely store work related information to minimize the risk of sharing material with other audiences outside of work.
- Storage devices should be secured to keys or similar valued items to reduce the risk of loss.

Even with the latter security in place the trust strongly advises staff to use the remote access provision as loss of personal data is likely to be viewed as a disciplinary offense as well as breaching GDPR compliance.

The use of mobile storage devices will be continued to be reviewed in line with the rest of this policy and the trust/individual schools reserve the right to change the policy at any time.

At no point, trust owned or personal, should any “jailbroken” or “hacked” device be connected to the trust network.

If employees require advice on how to protect data on mobile storage devices, they should contact a

member of the ICT service team.

Appendix G – Network usage and Access Guidance

Moving of equipment

- Hardware (including keyboards/mice/printers) should not be moved. It is acceptable to adjust computer settings for comfort and ease of use (but these must be adjusted back after use for the next user).

Usernames, passwords and logging on to the system

- Employees must not disclose your login username and password to anyone unless directed to do so by a member of the SLT for monitoring purposes or as stated earlier in this policy. Any member of staff viewing or caught trying to gain access to another member of staff's accounts, files or data will be subject to disciplinary action.
- Employees will be required to change your password in accordance with the login prompts. Ensure that you create appropriate passwords as directed. Do not write passwords down where they could be used by another individual.
- Employees, before leaving a computer, are expected to log off and ensure the logging off procedure is complete before you leave. If you are moving away from a PC for a short period of time use the Windows + L command to lock the computer. Projectors are expected to have been switched off when employees leave.
- Employees must not use any hardware/software under the username/profile of another employee. This includes Arbor/email/the network.

Remote access

Remote access is provided to employees to create more flexibility in their work (should they wish to use this). Expectations in relation to employees use of remote access include:

- Only using trust-provided hardware or password protected (secure) personal devices to access the network.
- Ensuring that any device used to access the network has up-to-date anti-virus software installed (to protect both your device and the trust network from harm)
- Logging in and out using the agreed protocols (this includes it being the employee's personal responsibility to log out of software applications to allow fair access to others).
- Ensuring that remote access is undertaken in a private space/area/location and that non-employees (for example family members*) do not and cannot view or access trust systems/data or the personal information of other employees or students.

Appendix H – reporting concerns and policy compliance

- Malfunctions or technical issues must be reported to the designated ICT support team as soon as they are found via the specified contact details.
- Suspected breaches to this policy should be reported to a member of the on-site SLT of each school who will take the lead in deciding any action that needs taking.
- Employees should be aware that this policy is part of a wider range of policies and support

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

documents (some external to school) that employees are expected to adhere to to fulfill their statutory and contractual obligations.
Examples of related policies/guidance include:

- Keeping Children Safe in Education
- The General Data Protection Regulations
- DMAT disciplinary policies
- DMAT Equality policy
- A range of wider UK laws
- Regulatory body laws e.g. copyright law

- If an employee breaches this ICT policy, they may also be in breach of further policies and/or the law and any action taken may just be limited to that by DMAT. Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

Appendix I: Student ICT usage agreement^

Name…… Form class……

Information Communication Technology (ICT) is part of everyday life. It supports work, learning and communication. This document sets out the clear expectations for DMAT in relation to ICT. It will keep students safe, well-informed and encourages respect for others in our community and school. Any breaches of this document are also a breach of the school's behaviour policy and are likely to result in sanctions. The final decision rests with the school; if you are unsure about any statement in this document, ask.

This usage agreement sets out the expectations of all students when they are both using:

- Trust owned/provided ICT
- Their personal ICT (when this is used to either communicate with other members of the school community or publish any form of information in relation to it as an organization or individual employees; irrespective of the timing of this use)

ICT (hardware & software, onsite and virtual) is provided by the trust for students to use to support their learning. Thus, all students, at all times, are expected to use trust provided ICT solely for the purposes of learning and communication in relation to school matters/events.

Students must never:

- Access the ICT network or system using anyone else's account or login information or share your own username and/or password with any other student. In addition, students should avoid writing down their usernames/passwords.
- Leave any device on which you are logged into "open" when you are not using it. Always use Windows + L keys (or equivalent) to lock your machine when not working at it and fully log off when you are finished.
- Cause damage to or attempt to move/change/remove or hack into any school ICT or other students/employees accounts. This includes the entirety of the trust's virtual environments/storage facilities.
- Install/download software, games and/or applications onto trust ICT.
- Give out personal information to other people you don't personally know via electronic devices/social media. It is an expectation (and good practice) that all students use the privacy settings to keep private information private!
- Use the trust's networks or any other ICT (this includes hardware e.g. mobile phones and/or software/social media) to post, share or communicate any images, comments or material* that is:
    - Illegal e.g. pornographic,
    - Harmful or hurtful in any way to any other person.
    - Racist or homophobic
    - Perceived to be of a bullying nature (see behaviour policy appendix for more details)

  This includes the publishing/posting of anything on social media (e.g. snapchat, Instagram or WhatsApp*) that would damage the reputation of the school/trust. This also includes times when students are not in school.
- Use a camera or any other recording device (audio or visual) in school/whilst on a school trip without first having the permission of a member of staff.
- Use of recording device in toilets or changing rooms, regardless of intent, will be treated as a serious violation breach of this agreement and it is likely very serious sanctions up to and including permanent exclusion will be considered.
- Record staff/other students outside of school without their explicit permission. At no time will it be

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

acceptable to share on any form of social media or device any recording (audio, photo or video) of members of staff.
- Open attachments or click on links if they are unsure of the source or attempt to spread viruses or other harmful content.
- Use mobile phones and/or any other electronic devices/accessories (for example* smartwatches, portable gaming devices, music playing devices, tablets, headphones, Bluetooth speakers) on the school site.

(Smartwatches are defined as any device that can send/receive calls, messages or similar via WIFI/3G/4G/5G or Bluetooth)

The school accepts no responsibility for the loss of damage to any mobile ICT device or other expensive items that students choose to bring on site.

Students who do not comply with this policy (whether this takes place within school/using trust provided ICT equipment or outside of school) are in breach of this agreement and hence will face sanctions. These may be issued by the school and/or result in a report being made to an outside agency such as the police*. **ALL issues to do with social media use must be left at the school gate.**

As a general reminder to all students:

- Student safeguarding and wellbeing are two of our top priorities. These clear guidelines are given to support your safety and wellbeing.
- Staff are permitted to search and remove any material deemed as harmful from any mobile electronic device. Staff are also permitted to collect and confiscate mobile devices if it is believed material on them is illegal or harmful.
- Staff are also able to direct a student to remove any material deemed not appropriate, whether this is on an external website.
- All activity that takes place across trust networks is tracked and monitored. This includes use of the WIFI as well desktop computer use. All material (internet sites) viewed, words typed, files stored, or information sent/published/uploaded is tracked and should not be considered private.
- They are responsible for reporting damage to ICT facilities as soon as it occurs/is discovered. This can be done via any member of staff or direct to ICT services.
- The Connect, school email system, personal file storage area and remote access are provided to help you to be organized and keep up to date in your studies/learning and homework. It is expected students will regularly check their email and use Connect.
- If they are worried about anything in relation to the use of ICT by themselves or another student/adult, they should report this to a member of staff ASAP.
- IF using social media, you are responsible for sticking to the published rules of each site/piece of software used (including minimum ages and publication of content). As a general rule student should never take images/video or publish any information about another person without their permission.

Signed ……..

Date……

^note this agreement will be regularly reviewed and updated to keep you as safe as possible when online and ensure that the school's ICT is maintained in the best possible way to help you to learn.

*indicates lists are not exhaustive rather exemplars given to aid understanding in relation to the point being made

^ Headteacher should also be read as Co-Headteachers^

Appendix J: Associated documentation and policies

This policy should be read in conjunction with other trust policies including*:

- DHS Child Protection Policy
- DMAT Data Protection Policy
- DMAT Code of Conduct for Employees
- DMAT Staff Behaviour at Work Policy
- DMAT Disciplinary procedure incl. Allegations and concerns regarding staff (...)
- Copyright guidance
- DMAT staff privacy notice
- DMAT privacy notice for students
- Individual employee's contract of employment
- Home-school agreements

User checklist:

1. I am aware and understand that anything I do when using a school device/network can and will be subject to monitoring via school software (this includes personal information viewed on school devices on home networks e.g banking/personal emails).
2. I am aware that, at all times, I am responsible for maintaining security to prevent third party access/sharing of school data and information.
3. I am aware that, if I use social media, I am responsible for what I post and I am expected to maintain trust in the profession.
4. I am aware that I am responsible for maintaining professional communication when using ICT. Specifically, that my communication with colleagues and any other third party on behalf of of the school needs to adhere to expectations and designated times.
5. I am aware and understand that if I breach the expectations as set out in this policy I could be subject to disciplinary action.