ICT ACCEPTABLE USE POLICY

Author:	Governance and Compliance Manager
Approval needed by:	Chief Executive
Consultation required	Trust ICT Team and DPO
Adopted (date):	25th June 2021
Date of next review:	As and when required

Why have an ICT Acceptable Use Policy?

An ICT Acceptable Use Policy is about ensuring that you, as a student, member or staff or volunteer at The de Ferrers Trust (the Trust) can use the internet, email and other technologies available at our academies in a safe and secure way.

The policy also extends to out of school facilities i.e. equipment, printers and consumables, internet, social media, email, managed learning environments, cloud services and websites.

We will use the term ‘users’ throughout this policy to cover staff, students volunteers including members, Trustees, local governors and clerks.

An ICT Acceptable Use Policy also sees to ensure that you are not knowingly subject to identify theft and therefore fraud. Also, that you avoid cyber-bullying and just as importantly, you don’t become a victim of such abuse. We have also banned certain sites which put the Trust network at risk. Help us, to help you keep safe.

The Trust strongly believes in the educational value of ICT and recognises its potential to enable all users in delivering and supporting the curriculum. The Trust also believes that it has a responsibility to educate its students; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and other related technologies. To this end the expectation of the Trust is that all users will play an active role in implementing the Trust’s ICT Acceptable Use Policy.

The Trust recognises that for all users to effectively deliver and support the curriculum they must be able to make use of the ICT facilities available and have the opportunity to expand and develop the material associated with their work. However, the Trust expects that all users, will at all times, maintain an appropriate level of professional conduct in their own use of our ICT facilities.

Listed below are the terms of this policy. All users are expected to use the ICT facilities of the Trust in accordance with these terms. Violation of these terms is likely to result in disciplinary action in accordance with the Trust’s Disciplinary Policy.

A summary of ICT Acceptable Use Policy key points will be displayed in classrooms, offices and on network machines.

Please read this document carefully and sign and date the appropriate declaration to indicate your acceptance of the terms herein.

Equipment

Computers

All computers and associated equipment are the property of The de Ferrers Trust and must be used in accordance with this policy which adheres to the Computer Misuse Act 1990, Data Protection Act 2018 & the GDPR 2018. The Trust’s ICT Team assumes responsibility for maintenance of all hardware and software. Mis-use of equipment includes, but is not limited to the following:

- Modification or removal of software
- Unauthorised configuration changes
- Creation or uploading of computer viruses or other malware
- Deliberate deletion of unuthorised/inappropriate files without permission
- The uploading of unuthorised/inappropriate computer files to the Trust's network

Any of these actions reduces the availability and reliability of computer equipment, puts other users' data at risk and increases downtime caused by repairs, thus delaying other essential work such as upgrades or enhancements.

Portable devices

Portable devices such as tablets are issued to all staff as required. Portable devices remain the property of the Trust all times, and their usage is subject to the following guidelines:

- The equipment remains the property of the Trust at all times and must be returned to the Trust at the end of the contractual period.
- Maintenance of the equipment is the responsibility of the Trust. All maintenance issues must be referred to ICT Support through the usual channels.
- All installed software must be covered by a valid license agreement held by the Trust.
- All software installation must be carried out by ICT Support in accordance with the relevant license agreements.
- Users may be allowed to download/install/uninstall some apps on tablets in accordance with settings on the Mobile Device Management (MDM) systems.
- No software should be removed, uninstalled or disabled under any circumstances. Any software problems should be reported through the usual support channels.
- Antivirus software must be updated regularly. For laptop computers, it will be necessary to connect them to the Trust network or Internet to update the antivirus software. This should be done at least weekly.
- The user of the equipment is responsible for all personal files and data stored on the equipment. Backup of the data is the responsibility of the user. It is strongly recommended that all data is regularly backed up, either to secure cloud-based services (eg, Google Drive or iCloud,) or to the Trust's network. Where removable media is used the user must ensure that such media is encrypted and has not been used to download materials that are at risk of damaging the network. The Trust's ICT team can transfer files for users if they are experiencing difficulties or in urgent situations.
- The user of the equipment must not encrypt any data or password protect any files that may prevent any future usage of the equipment. The encryption of hardware will be undertook/supervised by the Trust's ICT team.
- Some staff may need to encrypt or password protect specific files of a personal nature (eg, medical records or safeguarding concerns)
- The Trust cannot be held responsible for loss of data in the event of either a hardware or software failure or user error.

- From time to time, it may be necessary for the Trust's ICT team to perform software updates and maintenance for which the equipment must be made available/handed in when reasonably requested.

Use of removable storage media

Staff/ Volunteers/Members/Trustees/Local Governors and Clerks

All use of removable media must be agreed by Trust leadership in discussion with the Trust's ICT team. This needs to be considered on an individual basis. All users will be directed to use their secure Google account, were possible, as it limits file sharing to users within the @deferrers.com or @deferrersTrust.com domain.

Students

Whilst students may use removable memory devices to transfer files between home and their academy, the Trust cannot guarantee the correct operation of any removable media or the integrity of any data stored on it. The Trust cannot guarantee the correct operation of removable memory devices on the system, although every effort is made to ensure that this facility is available. Students are advised to use Trust Google Drive or iCloud for file transfer between academy and home where possible.

Printers

Printers are provided across the Trust for educational or work-related use only. All printer usage can be monitored and recorded.

- Always print on a black & white printer unless colour is absolutely essential
- Proof-read your document on-screen and use the 'Print-Preview' facility to check the layout before printing.
- Do not print unnecessarily or waste ink or paper.
- Avoid printing directly from websites where possible. Website pages are often not suitably formatted for printing and may cause wastage of paper and other consumables.
- Do not print sensitive information where possible. If you do have to print it, send it to a print queue and then release it from a copier when you are present using your cars/code number.

Data security and retention

All data stored on the Trust's network is backed up daily and backups are stored for up to a month online (using secure cloud services). If you should accidentally delete a file or files in your folder or shared area, please inform the Trust ICT team immediately so that it can be recovered. Generally, it is not possible to recover files that were deleted more than 1 month previously.

Google services such as Google Drive will not be part of the main Trust daily backups and users are encouraged to make use of Google Shared Drives to provide easier recovery of deleted files and ensure that key files do not disappear when staff leave.

Any iPad users should ensure that backups are regularly made to iCloud to allow for full recovery in the event of loss of data or content.

Internet & email

Content Filtering

The Trust provides Internet filtering, designed to remove controversial, offensive or illegal content. However, it is impossible to guarantee that all controversial material is filtered. If you discover any websites containing inappropriate or offensive content, please report these to the Trust's ICT team so that they can be added to filtering lists.

Acceptable use of the Internet

Use of the Internet should be in accordance with the following guidelines:

- Transmission of any material in violation of any United Kingdom or other national laws is prohibited. This includes, but is not limited to, copyrighted material, threatening or obscene material or material protected by trade laws
- Only access suitable material – Using the Internet to obtain, download, send, print, display or otherwise transmit or gain access to materials which are unlawful, obscene or abusive is not permitted.
- Respect the work and ownership rights of people outside the Trust. This includes abiding by copyright laws.
- Do not access internet chat/social networking sites without authorisation. These represent a significant security threat to the Trust's network.
- The use of unauthorised online gaming sites is prohibited. These consume valuable network resources that may adversely affect the performance of the system.
- Do not print out pages directly from a website. Web pages are often not suitably formatted for printing and this may cause significant wastage of paper. If you wish to use content from websites, consider using the copy and paste facility to move it into another application, copyright permitting.
- Do not attempt to download or install unauthorised software from the internet. The Trust's ICT team assumes responsibility for all software upgrades and installations.
- Staff are reminded that all internet access is logged and actively monitored and traceable.
- The duration of data being stored on the Trust's network is an issue that the Trust's ICT team will need to decide upon in conjunction with Trust leadership and the Data Protection Officer. This will be documented on the Trust's retention policy.

Email

Staff are provided with an email address by the Trust. This may be used for any legitimate educational or work-related activity. Staff should use the email in accordance with the following guidelines and are reminded that the Trust retains the right to monitor email communications at any time if this is deemed necessary:

- The sending or receiving of messages which contain any inappropriate material is strictly forbidden. This material includes, but it not limited to, pornography, unethical or illegal requests, racism, sexism, inappropriate language, or any other use which may be likely to cause offence. Disciplinary action will be considered in all cases.

- Messages relating to, or in support of any illegal activities may be reported to the authorities.
- Whilst it is possible to attach files to an email message, staff are advised that that email is not generally suited to transferring large files. Whilst there are no hard and fast rules regarding file sizes that can be attached to an email message, files exceeding approximately 25MB in size are generally considered to be excessively large and staff should consider using other methods to transfer such files, such as sharing links to Google drive folders or iCloud collaboration.
- Do not download or open file attachments unless you are certain of both their content and origin. File attachments may contain viruses or other forms of malware that may cause loss of data or damage to the Trust's network.
- Staff should not send personally identifiable information by email, as it is not a secure medium.
- You should only use the Trust's e-mail system for Trust related emails.
- Please see additional e-mail protocol document (Appendix 1) for other guidance in use of e-mail.

Trust's disclaimer

The Trust's e-mail disclaimer is automatically attached to all outgoing e-mails and you must not cancel or disapply it.

Monitoring

Copies of all incoming and outgoing e-mails, together with details of their duration and destinations are stored centrally (in electronic form). The frequency and content of incoming and outgoing external e-mails are checked from time to time to determine whether the e-mail system is being used in accordance with this policy and code of practice.

The Trust leadership team and the Trust's ICT team are entitled to have read-only access to your e-mails.

Security

As with anything else sent over the internet, e-mail is not completely secure. There is no proof of receipt, e-mails can be 'lost', they can suffer from computer failure and a determined 'hacker' could intercept, read and possibly alter the contents.

As with other methods of written communication, you have to make a judgment about the potential damage if the communication is lost or intercepted. Never send bank account information, including passwords, by e-mail.

Where possible, anonymise reference to staff or students in e-mails of a confidential nature and double check who is receiving them.

Program files and non-business documents

You must not introduce unauthorised program files or non-business documents from outside onto the Trust's network. This might happen by opening an e-mail attachment or by downloading a file from a web site. Although virus detection software is installed, it can never be guaranteed 100% successful, so introducing nonessential software is an unacceptable risk for the Trust. If you have any reason for suspecting that a virus may have entered the Trust's systems, you must contact the Trust's ICT team immediately.

Viruses

If you suspect that an e-mail has a virus attached to it, you must inform the Trust's ICT team immediately.

Spam

You must not send spam (sending the same message to multiple e-mail addresses) without the permission of senior staff.

Further guidance regarding email

All users should be guided by the following good practice:

- All users should check their e-mails on a daily basis and respond, as appropriate, within a reasonable period if the e-mail is directly addressed to them
- All users should avoid Spam.
- All users should avoid using the e-mail system as a message board and thus avoid sending trivial global messages. Whilst accepting the convenience of the distribution lists, all users should try to restrict its use to important or urgent matters.
- All users should send e-mails to the minimum number of recipients
- All users are advised to create their own distribution lists, as convenient and appropriate
- All users should always include a clear subject line
- All users are advised to keep old e-mails for the minimum time necessary
- Remember: E-mails remain a written record and can be forwarded to others or printed for formal use
- As a rule of thumb users should be well advised to only write what they would say face to face, and should avoid the temptation to respond to an incident or message by e-mail in an uncharacteristic and potentially aggressive fashion. Remember "tone" can be misinterpreted on the printed page and once it is sent it could end up in the public domain forever. Email lacks the other cues and clues that convey the sense in which what you say is to be taken, and you can easily convey the wrong impression.
- Remember that sending email from your Trust account is similar to sending a letter on Trust letterhead, so don't say anything that might bring discredit or embarrassment to yourself, your school or the Trust.
- Linked with this, and given the popularity and simplicity for recording both visual and audio material, users are advised to remember the possibility of being recorded in all that they say or do.

Educational use of Videoconferencing and/or Webcams

- The de Ferrers Trust recognise that videoconferencing and use of webcams can be a challenging activity but brings a wide range of learning benefits.
    - All videoconferencing and webcam hardware will be switched off when not in use and will not be set to auto-answer.
    - The Trust will primarily use Zoom as a videoconferencing tool, although staff/students may be required to use other such as Webex, Teams and Google Meet for specific activities or external meetings
    - Videoconferencing contact details will not be posted publicly.
    - Staff will ensure that external videoconferencing opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.
    - Any external Video conferencing equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use~~.~~

Users

- Videoconferencing or live video lessons will be supervised appropriately, according to the learner’s age and ability. See additional guidance on use of Zoom for video lessons.
- Any external video conferencing will take place via official and approved communication channels following a robust risk assessment.
- Only key administrators will be given access to videoconferencing administration areas or remote-control pages (ICT technicians and ALT i/c learning technologies)
- Any meeting links and password details for the videoconferencing services will only be issued to members of staff and should be kept securely, to prevent unauthorised access.

Content

- When recording a videoconference lesson, it should be made clear to all parties at the start of the conference and the reason for the recording must be given and recorded material will be stored securely, usually in Zoom or Google Drive cloud storage areas.
- If third party materials are included, we will check that recording is permitted to avoid infringing the third-party intellectual property rights.
- We will establish dialogue with other conference participants before taking part in a videoconference; if it is a non-educational site, staff will check that the material they are delivering is appropriate for the learners.

Management of online platforms

- The de Ferrers Trust uses Google Suite in all academies as its official online platform for communication, file sharing and productivity.
- Academy Leadership Teams/ICT Technicians will monitor the usage of Google Suite tools, including message/communication tools and publishing facilities.
- Only current members of staff and students will have access to Google Suite

- When staff and learners leave the setting, their account will be disabled. Learners and staff will be advised about acceptable conduct and use when using Google Suite
- All users will be mindful of copyright and will only upload appropriate content onto Google Suite. External sharing links outside of @deferrers.com or @deferrersTrust.com addresses are blocked
- Any concerns about content on Google Suite tools will be recorded and dealt with in the following ways:
  - The user will be asked to remove any material deemed to be inappropriate or offensive.
  - If the user does not comply, the material will be removed by the site administrator/ICT technicians.
  - Access to Google Suite for the user may be suspended.
  - A student's parents/carers may be informed.
  - If the content is illegal, we will respond in line with existing child protection procedures.
- Learners may require editorial approval from a member of staff. This may be given to the learner to fulfil a specific aim and may have a limited time frame.
- A visitor may be invited into Google Drive by a member of Leadership Team, for example those conducting an inspection or audit. In this instance, there may be an agreed focus or a limited time slot during which an account is active.

Management of Applications (apps) used to Record Children's Progress

- We use SIMS as an MIS and related apps to track learners progress and share appropriate information with parents and carers.
- The Principal is ultimately responsible for the security of any data or images held of children. As such, they will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulations (GDPR) and Data Protection legislation.
- A backup of all MIS data will be collected overnight and stored securely via RedStore cloud backup solution.
- To safeguard students' data:
  - Only students issued devices will be used for apps that record and store learners' personal details, attainment or photographs.
  - Staff will be issued a login for SIMS/other apps as required, with access and functionality appropriate for their role and position within the academy
  - Personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store learners' personal details, attainment or images.
  - Devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft.
  - All users will be advised regarding safety measures, such as using strong passwords and logging out of systems.
  - Parents and carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images.
  - Staff will be expected to clear old data as part of a data purge, in line with current data storage/retention guidelines

USE OF PERSONAL DEVICES AND MOBILE PHONES

The de Ferrers Trust recognises that personal communication through mobile technologies is an accepted part of everyday life for learners, staff and parents/carers, but technologies need to be used safely and appropriately within the setting. Each academy will have its own mobile phone policy that students will adhere to and parents/carers will be made aware of, along with appropriate sanctions for misuse.

Staff Use of Personal Devices and Mobile Phones

- Staff should not use personal mobile devices in areas of the academy where phones are not allowed, including in lessons.
- Staff should not take images of students on mobile phones, but use devices provided by the academy such as their iPad. If photos are taken, for example on an educational visit for posting on social media, the images will be forwarded to the correct person and deleted from the device afterwards, unless this has been approved in advance by the academy Principal for appropriate reasons

Learners' Use of Personal Devices and Mobile Phones

- Learners will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.
- For students at secondary academies, their personal devices and mobile phones are expected to be:
  - kept in a secure place, kept out of sight during lessons and while moving between lessons
  - used only in approved areas.
- If a student needs to contact his/her parents or carers they will be allowed to use an academy phone via Reception or relevant Student Support Team.:
  - Parents/carers are advised to contact their child via Reception; exceptions may be permitted on a case-by-case basis.
- Mobile phones or personal devices will not be used by students during lessons or formal educational time unless as part of an approved and directed curriculum-based activity with consent from a member of staff.
  - The use of personal mobile phones or devices for a specific education purpose does not mean that blanket use is permitted.
- Mobile phones and personal devices must not be taken into examinations.
  - students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.
- If a learner breaches the policy, the phone or device will be confiscated and will be held in a secure place for the remainder of the day.
  - Staff may confiscate a learner's mobile phone or device if they believe it is being used to contravene our behaviour or bullying policy or could contain youth produced sexual imagery (sexting).
  - Searches of mobile phone or personal devices will only be carried out in accordance with DfE guidance and our policy.

    - Students mobile phones or devices may be searched by a member of the leadership team, student support team or a progress leader with the consent of the student or a parent/ carer. Content may be deleted or requested to be deleted, if it contravenes our policies.
    - If there is suspicion that material on a learner's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation.

Visitors' Use of Personal Devices and Mobile Phones

- Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: anti-bullying, behaviour, child protection and image use.
- We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.
- Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL (or deputy) or Principal of any breaches our policy.

Officially provided mobile phones and devices

- Some members of staff may be issued with a work phone, where contact with students or parents/carers is required.
- Academy mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.
- Setting mobile phones and devices will always be used in accordance with the acceptable use policy and other relevant policies.

External services

The Trust provides a number of services that are accessible externally, using any computer with an Internet connection. These should be used strictly for educational or work-related activities only and in accordance with the following guidelines.

Users using their own facilities at home should abide by the principles and practices on safe and secure Internet practice and use of email, as set out in this policy.

Privacy and data protection

<u>Passwords</u>

- Never reveal your password to anyone else or ask others for their password.
- When choosing a password, choose a word or phrase that you can easily remember, but not something which can be used to identify you, such as your name or address. Generally, longer passwords are better than short passwords. It is advisable to use a 'strong' password. A strong password is one which contains a combination of upper and lower-case letters, numbers and other punctuation characters. You can substitute numbers and letters for other characters that look similar, such as '3' for 'E', '1' for 'I' or '@' for 'O', '!' for '1' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.

- If you forget your password, please request that it be reset via the Trust ICT team.
- If you believe that someone may have discovered your password, then change it immediately.

Security

- Never attempt to access files or programs to which you have not been granted authorisation. Attempting to bypass security barriers may breach data protection regulations and such attempts will be considered as hack attacks and will be subject to disciplinary action.
- You should report any security concerns immediately to the Trust's ICT team.
- Any user identified as a security risk will be denied access to the system and subject to disciplinary action in accordance with Trust's disciplinary procedures.

Management and Information Systems

Access to MIS software [e.g. SIMS.net] is available only from designated locations and only to those staff who require it. Access is subject to approval from the Trust's leadership team. Usage of MIS software is subject to the following guidelines:

- Password security is vital. If you believe that your password has been discovered change it immediately.
- If you leave your computer or device unattended, particularly in a classroom, either log out or lock it by using the CTRL-ALT-Delete keys and then choosing "Lock Workstation". Once this is done, you will need to re-enter your password to gain access to the computer.
- If you are using MIS software on a computer in a classroom connected to an interactive whiteboard and projector, please be aware that any student information you display on your screen may also be displayed on the whiteboard if the projector is turned on. To ensure protection of sensitive data, pleas ensure that projectors are turned off or disconnected before using MIS software.
- Joining administration and curriculum networks raises issues regarding who within the organisation has access to data. Within the Trust it is understood that the Trust's leadership team have a clear duty of care to protect the access to confidential data.
- Where staff are working at home and connect remotely to the Trust's MIS system then all of the above considerations also apply. Staff must ensure that their home Internet connection is secure from outside access particularly if a wireless network is used. Additionally staff should take due care of any material which they print at home.
- Remote access to MIS will normally be limited to approved key individuals within each academy, including leadership teams and heads of year.

Mobile technologies

For reasons of safety and security staff, volunteers, members, Trustees, local governors and clerks should not use their mobile phone or any other technology in a manner that is likely to bring the Trust into disrepute or risk the welfare of a child or young person.

The development of mobile technology is such that mobile phones and other similar devices connected to mobile networks have enhanced features which include: picture messaging; mobile access to the internet; entertainment in the form of video streaming and downloadable video clips from films, sporting events, music and games etc. The capabilities of mobile phones also means that adults working within the school environment may be sent inappropriate images or videos, or be encouraged to send back images or video of themselves using integrated cameras.

In order to reduce the opportunity for those behaviours that could possibly cause upset, it is advisable that staff, members, Trustees, local governors, clerks and volunteers working with children and young people within the school setting, limit their use of mobile technologies to necessary communication during specified breaks during the school day. If you are sent inappropriate material e.g. images or videos report it immediately.

If staff need to take photographs or video recordings of events, students, displays, work, then this should be done using their academy devices, not their own personal devices.

Support services

All ICT hardware and software maintenance and support requests should be submitted to Trust's ICT team using one of the following methods:

- E-mail to the relevant accounts for reporting faults
- Phone the appropriate member of the ICT technical team

The Trust will make every effort to ensure that all technical or operational problems are resolved within a reasonable time.

Software installation

The Trust's ICT Team assumes responsibility for all software installation and upgrades. Users may request the installation of new software packages onto the network, but this will be subject to the following:

- A minimum of 5 working days is required for packaging and installation of new software.
- Software cannot be installed on the Trust's network without a valid license agreement. This must be supplied with the software package.
- Please check the licensing terms of the software package carefully to ensure that it is suitable for use on the Trust network. If you are unsure, please ask Trust ICT for assistance. A relevant and valid license agreement document will be required before any software packages can be installed.
- All software installation media and license agreements are held centrally within the Trust to aid in license tracking and auditing. Installation media cannot normally be released except by special agreement.
- When purchasing new hardware or software for use on the Trust network, please check its suitability, compatibility and licensing terms with the Trust's ICT team before any purchases or agreeing any contracts. Purchase orders for new hardware and software will normally be authorised only with the agreement of Trust ICT team and the Trust finance team.

Service availability

Whilst every effort is made to ensure that the systems, both hardware and software are working correctly, the Trust will not be responsible for any damages or loss incurred as a result of system faults, malfunctions or routine maintenance. These damages include loss of data as a result of delay, non-deliveries, mis-deliveries or service interruptions caused by the system or elements of the system, or your errors or omissions. Use of any information obtained via the Trust ICT system is at your own risk. The Trust specifically denies any responsibility for the accuracy of information obtained whilst using the Trust systems.

Social media

In order to protect our students, staff and the reputation of the Trust, along with the Social Media Policy, we have provided clarification of guidance and common sense rules to follow when using social networking sites for private use, to ensure that your private social networking does not compromise your professional position.

If you are responsible for a social media account on behalf of the Trust, it will be necessary to hold the details of the account including password centrally for safety purposes. Please provide these to [insert contact here]

You should:

- Act in accordance with the Trust's ICT policy and this Acceptable Use policy
- Always make sure that you log out after using social networking sites. If you don't, another person may access your account and post something under your name.
- Be aware that the Trust may monitor your social media usage, in and out of work.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation/UK GDPR requirements.
- Stop the network provider (ISP) from passing on your details to other companies for research and advertising purposes. For example, to stop Facebook from forwarding your details, click 'Privacy Settings'. under 'Applications and websites' click 'edit your settings'. Scroll down to 'instant personalisation' and make sure the checkbox for 'enable instant personalisation on partner websites' is unchecked.
- Ensure your privacy and security settings on your profile are set to a high level, or it may open your content to a large group of unknown people and your privacy may be at risk.
- Notify your line manager straight away if you think you are a victim of cyber bullying or offensive messages. The Trust takes cyber bullying and the welfare of its staff very seriously and will address the matter accordingly. If you believe a social networking account has been hacked, contact the company immediately & report it.
- Remember that even after a post is deleted or removed, it may still be available to view as a screenshot, etc.
- Remember, people classed as 'friends' have the ability to view and share your information with others. Only post what you are happy for the world to see. Imagine your students, their parents and your colleagues viewing your post and think if you would be happy for them to read it. If the answer is no, don't post it.
- You should ensure that photographs or videos in which you appear are appropriate. Other users could post a photograph of you on their profile in which you are named. If you do find that you are 'tagged' or named in a photograph, remove the tag, contact the person and ask them to remove all references to you

in the photograph. Most social networking sites also allow you to report images you are unhappy with.

- If your duties require you to speak on behalf of the Trust, in a social media environment, you may be required to undergo training before you do so and certain requirements and restrictions may be imposed with regard to your activities.
- Likewise, if you are contacted for comments about the Trust or any of our academies for publication anywhere, including in any social media outlet, direct the inquiry to Trust leadership and do not respond without written approval.
- If you disclose your affiliation as an employee of the Trust, you must also state that your views do not represent those of your employer. For example, "the views in this posting do not represent 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 pupils, parents and colleagues.

You must NOT:

- Post photographs or videos of other staff without their permission
- Make disparaging remarks about your employer, colleagues, students, suppliers and other stakeholders on social networking sites, or say anything online that could bring the Trust into disrepute.
- Use the Trust name, name of any academy, logo or branding. In specific examples you may be given permission from the Trust to set up official academy social networking accounts (eg, Twitter, Instagram, Facebook). In these circumstances, you must give login access to 2 or 3 staff, to provide transparency, and provide password details to the Trust leadership team to be recorded centrally.
- Access personal social networking sites during working hours.
- Accept any students as friends or followers (including sixth form). We recommend that you also not accept parents of students as friends or followers.
- Discuss students, colleagues or the Trust online, either in the public domain or in a private message / conversation.
- Talk to students online, in the public domain or a private message / conversation. You might use official academy/Trust social networking sites to communicate with students in a professional manner (eg, to answer specific faculty questions) where it is appropriate and permission to use such an account has been given, as stated above.
- Write anything on social networking sites that you would not want the world to see. Students, other staff and parents may access your profile and could complain to the Trust if your profile contains offensive comments or photographs. Remember, posts on social networking sites are documented and once written and published, they cannot be retracted.

Useful information

This policy has been written with the following legislation taken into consideration:

- Computer Misuse Act
- Data Protection Act 2018
- RIPA – Regulation of Investigatory Powers Act 2002
- UK GDPR – General Data Protection Regulations - 2018

Appendix 1 – E-Mails

E-Mail - Protocols

Please use the following common-sense guidelines:

- Check who the e-mail is sent to – any account with a 4-digit number (eg, *jsmith1234*) will be a student

- Only copy other staff in as required, avoid blanket ‘CC ’mails for everything.

- Please consider the content of any messages sent or forwarded, especially if it contains personal/sensitive data (GDPR compliance).

- Always write all e-mails in a professional & courteous manner, as expected by any large business organisation. Avoid comments that are unprofessional or insulting.

- Avoid the use of emojis and gestures which could be misconstrued by audiences (eg kisses).

- Use group lists wherever possible, to avoid sending unnecessary ‘all staff ’e-mails.

- Where possible, use the bulletin to distribute information that does not need to be sent via e-mail to reduce the volume in people’s inboxes.

- Try to use appropriate headers, eg, “*URGENT - READ*” “*ACTION REQUIRED*” or "*For teachers of Year 9* ” so it is easy to tell what the message is about.

- Do NOT use the Academy e-mail system and e-mail group lists to sell items or for private business interests. This is not allowed.

- DO use e-mail to contact individual students or your teaching groups, but only use your Academy e-mail address to do so. NEVER use your private e-mail for contacting students or parents. If staff receive an e-mail from a student that indicates emotional support is required this must be disclosed to a member of the safeguarding team. Under no circumstances should a member of staff attempt to counsel a student via e mail.

- Please put messages about social events and charity activities in the bulletin.

- Please do NOT assume that staff will be able to respond to all message during the day or in the evenings. Where possible, schedule e-mails to send after 08:00 and before 18:00, especially ALLSTAFF or FACULTY group mail.

- Staff are not expected to read or send e-mails outside of normal working hours.

- If you know you will be away for a period of time, set an ‘Automatic reply’

- Please think before you click SEND – Is the message appropriate? Is it necessary?

Quality

E-mails constitute records of the Trust and are subject to the same rules, care and checks as other written communications sent by the Trust so, for example:

- You should always consider whether it is appropriate for material to be sent to third parties;
- they may have to be disclosed in legal proceedings;
- they may have to be disclosed to a person if they makes a request to see information held about them under data protection law;
- they require the same level of authorisation before being sent;
- printed copies of e-mails need to be retained in the same way as other correspondence;
- they are confidential to the sender and recipient, unless you have been given permission to read them;
- transmitting the works of others, without their permission, may infringe copyright;
- sending or storing messages or attachments containing statements which could be construed as improper, abusive, harassing the recipient, libelous, malicious, threatening or contravening discrimination legislation or detrimental to the Trust is a disciplinary offence and may also be a legal offence.

Inappropriate e-mails or attachments

You must not use e-mail to access or send offensive material, chain messages or list-servers or for the purposes of bullying or plagiarising work.

You must not send personal or inappropriate information by e-mail about yourself, other members of staff, students or other members of the Trust community.

If you receive any inappropriate e-mails or attachments you must report them to the Trust’s ICT team.