



Policy Crib Sheet School: Excelsior MAT

Policy: ICT, Internet, Office365 and Social Media Networking Policy

Details:

Changes to the policy (Red removed, yellow replaced, green added):

5. PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY
 - Unauthorised e-mail attachments are automatically blocked. **Any such e-mail is sent to the IT Systems Manager who will then report to the student's Head of Year.**
 - **Changed to:** Unauthorised e-mail attachments are automatically blocked.
 - E-mails containing offensive language are automatically blocked. **Any such email is sent to the IT Systems Manager.**
 - **Changed to:** E-mails containing offensive language are automatically blocked as per our word list. This can be updated on request.

12. SECURITY

Added: It is required that staff undertakes at least once a year GDPR and Cyber Security training provided by the school and IT Team. If the member of staff requires a knowledge refreshment, the training can be reviewed through the year as many times as needed.

Added under Cloud Storage section: When sharing information from personal OneDrive, regardless of how this is shared or to whom, users must enforce a time limit of no longer than 1 month (30 days). This is set under the 'Set expiration date' option.

Added:

17. REPORTING INCIDENTS

When reporting IT incidents regarding devices, subscriptions, applications or cyber risks, users are required to promptly notify the IT support team through the helpdesk system. This ensures that all issues are documented and addressed in a timely manner. Users should provide detailed information about the incident, including the nature of the problem, any error messages received, and the steps taken prior to encountering the issue. This helps the IT team diagnose and resolve the problem more efficiently. Additionally, users are encouraged to follow up on their reports if they do not receive a response within the expected timeframe. Maintaining clear and open communication with the IT support team is crucial for the swift resolution of incidents and the overall security and functionality of the IT infrastructure.

Date: 04/02/2025



ICT, Internet, Office365 and Social Media Networking Policy

Policy Lead: Fabian Olteanu
Dec 2024

1. POLICY STATEMENT

The purpose of this Policy is to set out the Trust's recommendations and requirements for the use of ICT facilities, social networking and social media by its employees. In doing so, the Trust seeks to achieve an appropriate balance in the use of all of this by staff, as employees, as educators and private individuals, but also, with professional reputations and careers to maintain, and contractual and legislative requirements to adhere to.

Whilst the Trust does not wish to discourage staff from using the ICT equipment and social networking sites on the Internet in their personal time, it does expect certain standards of conduct to be observed in order to protect the Trust and its reputation, and also to protect staff from the dangers of inappropriate use.

Excelsior Multi Academy Trust is committed to developing appropriate technology to ensure the efficient and effective provision of ICT facilities. To this end, staff and pupils are encouraged to develop ICT skills including effective and safe use of both the E-mail and Internet systems. All use of E-mail and Internet facilities by staff and pupils at The Trust must be in accordance with this policy.

Accessing social networking sites in working time or at any time working in the capacity as a Trust employee is strictly forbidden except when using such sites in a professional capacity i.e. investigating cyber bullying or updating official school accounts.

Excelsior Multi Academy Trust recognises that the internet provides unique opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, X, Blogs and Wikis. However, employees' use of social media can pose risks to the Trust's ability to safeguard children and young people, protect confidential information and reputation and can jeopardise compliance with legal obligations. This could also be the case during off duty time.

Employees using social media are also potentially at risk of others misunderstanding the intent behind online communications or blurring of professional boundaries between children and young people and their parents or carers. This policy therefore sets out the Trust's expectations regarding the use of social media.

To minimise these risks, to avoid loss of productivity and to ensure that IT resources and communications systems are used only for appropriate business purposes and that the use of personal devices does not have an adverse impact on the Trust and its Academies, the Trust expects employees to adhere to this policy.

2. ROLES AND RESPONSIBILITIES

Headteacher and Senior Leadership Team

- Should ensure that all existing and new staff are familiar with this policy and its relationship to the Trust's standards, policies and guidance on the use of ICT.

- Should provide opportunities to discuss appropriate social networking use by staff on a regular basis and ensure that any queries raised are resolved swiftly.
- Must ensure that any allegations raised in respect of access to social networking sites are investigated promptly and appropriately, in accordance with the Trust's Disciplinary Procedure and Code of Conduct & Disciplinary Rules. This is also expected of support staff.

Staff

- Should ensure that they are familiar with the contents of this policy and its relationship to the Trust's standards, policies and guidance on the use of ICT.
- Should raise any queries or areas of concern they have relating to the use of ICT facilities, social media or social networking sites and interpretation of this Policy, with their line manager in the first instance.
- Must comply with this policy where specific activities/conduct is prohibited.
- The Teachers' Standards state that "A teacher is expected to demonstrate consistently high standards of personal and professional conduct".

Trustees

- Must ensure that this policy is implemented
- Should ensure that their own conduct is in line with that expected of staff, as outlined in this policy.

3. ALLOCATION OF EMAIL ADDRESSES

Staff and pupils (if agreed with the school) will be given an email address and should regularly check their email accounts for new mail.

All email users will be issued with a unique login name and password. The user can change the password at any stage. Accessing the email system using another user's account without prior authorisation is a breach of policy and is likely to result in disciplinary action.

4. SCOPE AND PURPOSE OF THE POLICY

This policy deals with the use of ICT facilities, social networking and all forms of social media; including Facebook, LinkedIn, X, Wikipedia, all other social networking sites, and all other internet postings, including blogs.

It applies to the use of social media for both business and personal purposes, whether during working hours or otherwise. The policy applies regardless of whether the social media is accessed using each Academy's IT facilities and equipment or equipment belonging to members of staff.

This policy covers all employees working at all levels and grades. It also applies to consultants, contractors, casual and agency staff and volunteers (collectively referred to as staff in this policy).

Third parties who have access to the Trust's electronic communication systems and equipment are also required to comply with this policy

The term 'employee' or 'staff' covers all employees/staff of the Trust, including casual

staff, agency employees and ex-employees. Where individuals from partner organisations are involved in acting on behalf of the Trust, they will also be expected to comply with this Policy.

Social networking applications include, but are not limited to:

- Social Networking (e.g. Facebook, X, Instagram, Snapchat etc.)
- Micro-blogging applications (e.g. X, Yammer, FMyLife)
- Online discussion forums and opinion sites (e.g. Ning)
- Blogs (e.g. Blogger, LiveJournal, Xanga)
- Employee's that identify themselves as a member of the Trust will become a representative of the Trust and therefore should represent the Trust in a professional and positive manner.

Breach of this policy may result in disciplinary action up to and including dismissal. Disciplinary action may be taken regardless of whether the breach is committed during working hours, and regardless of whether the Trust's equipment or facilities are used for the purpose of committing the breach. Any member of staff suspected of committing a breach of this policy will be required to co-operate with investigations.

Staff may be required to remove internet postings which are deemed to constitute a breach of this policy. Failure to comply with such a request may in itself result in disciplinary action.

5. PERSONNEL RESPONSIBLE FOR IMPLEMENTING THE POLICY

The Trust Board has overall responsibility for the effective operation of this policy.

All managers have a specific responsibility for operating within the boundaries of this policy, ensuring that all staff understand the standards of behaviour expected of them and taking action when behaviour falls below its requirements.

All staff are responsible for the success of this policy and should ensure that they take the time to read and understand it. Any misuse of social media (including 'hacking' of or misuse of personal accounts) should be reported to the Headteacher or HR department.

The Trust encourages the use of Teams and e-mail as an essential means of communication for both staff and pupils. However, the use of e-mail does introduce its own problems and may compromise our network security if not used correctly. Therefore, the following guidelines must be adhered to:

- Pupils may only use their approved school e-mail account on the school system. The use of all personal e-mail accounts such as Hotmail and Yahoo Mail is not permitted.
- Pupils must report to a member of staff immediately if they receive any email containing offensive materials.

- Pupils must not reveal details of themselves or others in e-mail communication, such as address, telephone numbers, etc.
- The forwarding of chain e-mails is not permitted.
- Unauthorised e-mail attachments are automatically blocked.
- E-mails containing offensive language are automatically blocked as per our word list. This can be updated on request.
- E-mails should be written carefully and politely following the Rules and Etiquette expected.
- The use of all personal cloud accounts on work devices, such as but not only Microsoft, Hotmail, Yahoo Mail is not permitted.

6. COMPLIANCE WITH RELATED POLICIES AND AGREEMENTS

Social media should never be used in a way that breaches any of the Trust's other policies. If an internet post would breach any of the Trust's policies in another forum, it will also breach them in an online forum. For example, employees are prohibited from using social media to:

- Breach the Trust's obligations with respect to the rules of relevant regulatory bodies
- Breach any obligations they may have relating to confidentiality
- Breach Disciplinary Rules
- Defame or disparage the Trust or its affiliates, Trustees, pupils, parents and carers, staff, business partners, suppliers, vendors or other stakeholders
- Harass or bully other staff in any way
- Unlawfully discriminate against other staff or third parties or breach the equal opportunities policy
- Breach the Data Protection policy (for example, never disclose personal information about a colleague online)
- Breach any other laws or ethical standards (for example, never use social media in a false or misleading way, such as by claiming to be someone other than yourself or by making misleading statements).

Staff should never provide references for other individuals on social or professional networking sites, as such references, positive and negative, can be attributed to the Trust and create legal liability for both the author of the reference and the Trust.

Employees who breach any of the above policies will be subject to disciplinary action up to and including termination of employment.

7. RECOMMENDATIONS AND REQUIREMENTS FOR THE USE OF INTERNET AND ONLINE SOCIAL NETWORKS

The Trust has provided pupils and staff with internet access to assist in raising educational standards via improved teaching and learning facilities. Internet access is an entitlement for pupils who show a responsible and mature approach to its use.

In order to protect pupils from offensive materials and to maintain network integrity, the following guidelines must be adhered to:

- Pupils must not attempt to logon to any computer unless the room is being supervised by a member of staff. The use of computer systems without permission or for inappropriate purposes could constitute a criminal offence under the Computer Misuse Act 1990
- The IT Support team are responsible for installing all authorised applications. Do not attempt to download and install any programs from any website including search bars, screensavers and games. File sharing applications are strictly prohibited. Files held on the Trust network will be regularly checked
- Software must not be copied unless licensing allows this and copies must only be made by the IT Support team. All users must be responsible for reporting to the IT department any sites or materials that are deemed in conflict with this policy
- The download of internet-based music and video is not permitted by pupils unless they have authorisation from a member of staff
- Offensive materials must not be downloaded or copied to the Trust system under any circumstances. These materials include pornographic material, themes of a violent nature, incitement to racial hatred or other material related to extremism or radicalisation and drug related images
- If pupils discover unsuitable or offensive web sites, they must report it immediately to a member of staff
- The use of Trust computers by staff will be monitored all the time with regard to ensuring that the Trust's Policies are being complied with
- Pupils must not access or participate in any unregulated online Chat activities. Pupils may be asked to participate in audio and/or video online lessons, such as international school linkups, but these sessions will be strictly regulated by a member of staff
- School computer and Internet use must be appropriate to the pupils' education or to staff professional activity during lessons
- Personal use of email/Internet by staff during school hours should be agreed by their line manager
- Pupils should not partake in any financial transactions online. The school Internet or email facilities should not be used, by anyone, for gambling, personal or financial gain, political purposes or advertising. This policy should also be adhered to when accessing the schools systems outside of normal working hours (including from home)

Personal use of social media is never permitted during working time or by means of the Trust's computers, networks and other IT resources and communications systems.

Working in an educational setting with young people, staff have a professional image to uphold, and how individuals conduct themselves online, helps to determine this image.

Friends and befriending

- One of the functions of social networks is the ability to "friend" others, creating a group of individuals who share personal news and /or interests. The Trust advises that staff must not initiate or accept friendships with pupils, or pupils' family members/friends under any circumstances.

- Staff who maintain social networking friendships with work colleagues are required to adhere to the requirements below relating to content of interactions.

Content of interactions

- Staff are recommended to refrain from making reference on social networking sites to the Trust, its employees, pupils, and their families. If staff adhere to this recommendation, then the personal content of an individual's social networking memberships is unlikely to be of concern to the Trust.
- An exception to the above would be content which details conduct outside of employment which affects the individual's suitability to perform his/her work or is liable to damage the Trust's reputation.
- If employment at the Trust is referred to, then the information posted would need to comply with the conditions set out below:
 - Any references made to the Trust, its employees, pupils and their families, should comply with the Trust's policies on conduct/misconduct, equal opportunities, and bullying and harassment.
 - Staff must not post information on a social networking site which is confidential to the Trust, its employees, its pupils or their families.
 - Staff must not post entries onto social networking sites which are derogatory, defamatory, discriminatory or offensive in any way, or which have the potential to bring the Trust into disrepute.
 - Staff should not use the Trust logo on their own personal social networking accounts and should not post any photographic images that include pupils.
 - When posting any information onto a social networking site, staff are recommended to consider whether any entry they make puts their effectiveness to perform their normal duties at risk.
 - If individuals feel aggrieved about some aspect of their work or employment, there are appropriate informal and formal avenues, internally within the Trust, which allow staff to raise and progress such matters. Social networks are not the appropriate forum to raise such matters. Employees should discuss any concerns with their Headteacher/line manager in the first instance. Guidance is also available from the HR Department.
- Where staff use educational/professional networking sites as a professional resource, which are not available to the general public; it is acceptable to make reference to the Trust. The above conditions relating to content of postings/communications will still apply.
- When using X the Trust recommends staff should set up a separate account in order to X school related items and have an account name set up to reflect this.

8. RESPONSIBLE USE OF SOCIAL MEDIA

The following sections of the policy provide staff with common-sense guidelines and recommendations for using social media responsibly and safely and in order to protect staff and the Trust.

Employees' use of social media can pose risks to the Trust's ability to safeguard children and young people, protect the Trust's confidential information and reputation, and can jeopardise the Trust's compliance with its legal obligations. This could also be the case during off duty time.

Safeguarding children and young people:

- Employees should not communicate with pupils over social network sites and must block unwanted communications from pupils. Any attempted contact should be reported to the **Designated Senior Person** of the relevant Academy.
- Employees should never knowingly communicate with pupils in these forums or via personal email accounts
- Employees should not interact with any ex-pupil of the Trust who is under 18 on such sites.
- Communication with pupils should only be conducted through usual channels (such as staff appointed school email addresses). This communication should only ever be related to Academy business.

Protecting the Trust's reputation:

- Employees must not post disparaging or defamatory statements about the Staff or Trustees of the Trust, its pupils or their parents or carers or any other affiliates and stakeholders.
- Employees must not post disparaging or defamatory statements about the Staff or Trustees of the Trust, its pupils or their parents or carers or any other affiliates and stakeholders.
- Employees should also avoid social media communications that might be misconstrued in a way that could damage the Trust's reputation, even indirectly.
- Employees should make it clear in social media postings that they are speaking on their own behalf write in the first person and use a personal e-mail address when communicating via social media.
- Employees are personally responsible for what they communicate in social media. They should remember that what they publish might be available to be read by the masses (including the Trust itself, future employers and social acquaintances) for a long time.
- If employees disclose their affiliation as an employee of the Trust, they must also state that their views do not represent those of their employer.
- Employees should avoid posting comments about sensitive Trust - related topics, such as their performance.
- If employees are uncertain or concerned about the appropriateness of any statement or posting, they should refrain from making the communication until they discuss it with the Headteacher.
- If employees see content in social media that disparages or reflects poorly on the Trust or its stakeholders, they should print out the content and contact the Headteacher or the HR department. All staff are responsible for protecting the Trust's reputation.

Respecting intellectual property and confidential information:

- Staff should not do anything to jeopardise the Trust's confidential information and intellectual property through the use of social media.
- In addition, staff should avoid misappropriating or infringing the intellectual

property of other companies and individuals, which can create liability for the Trust, as well as the individual author.

- Do not use an Academy's logo, brand name, slogan or other trademark, or post any of the Trust's confidential or proprietary information without prior written permission.
- Copying or movement of confidential data to unsecure systems (personal email, unencrypted memory sticks) is not permissible and breaches data protection requirements.
- All USB storage devices are prohibited

Respecting colleagues, pupils, parents and carers, trustees and other stakeholders:

- Do not post anything that your colleagues or our pupils, parents and carers, Trustees and other stakeholders would find offensive, including discriminatory comments, insults or obscenity.
- Do not post anything related to your colleagues or the Trust's suppliers, vendors or other stakeholders without their written permission.

9. ACADEMY RELATED USE OF SOCIAL MEDIA

If an employee's duties require them to speak on behalf of the Trust in a social media environment, they must still seek approval for such communication from the Headteacher, who may require them to undergo training before doing so and impose certain requirements and restrictions with regard to the activities.

Likewise, if an employee is contacted for comments about the Trust for publication anywhere, including in any social media outlet, direct the inquiry to the HR department and do not respond without written approval.

10. RULES FOR EMAIL USE

- You must never send abusive emails, even as a joke.
- You must never send unsuitable emails or attachments, such as things of a racist, violent or sexual nature.
- Never send or forward chain letters or similar items. They often contain viruses.
- It is prohibited to use another person's account to send email.
- You must never make personal remarks about another person in your emails
- You may not use the Trust email system to spread rumours or gossip about other people
- Foul language must never be used

Good email etiquette

- DO ensure that you have a relevant 'Subject' Line
- DO be careful when replying to mailing list messages, or to messages sent to many recipients. Are you sure you want to reply to the whole list?
- DO remember to delete anything that isn't needed or is trivial

Bad email etiquette

- DON'T reply to an email message when angry as you may regret it later. Once the message has been sent you cannot retrieve it
- DON'T keep mail in your inbox longer than necessary, especially large attachments
- DON'T type in CAPITALS as this is considered to be SHOUTING. This is one of the rudest things you can do
- DON'T post your email address on websites and other public parts of the Internet unless you want to be deluged with spam

11. MONITORING

The contents of the Trust's IT resources and communications systems are the Trust's property. Therefore, staff should have no expectation of privacy in any message, files, data, document, facsimile, telephone conversation, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on each Academy's electronic information and communications systems.

Each Academy within the Trust reserves the right to monitor, intercept and review, without further notice, staff activities using its IT resources and communications systems, including but not limited to social media postings and activities, to ensure that rules are being complied with and for legitimate business purposes and employees consent to such monitoring by acknowledgement of this policy and use of such resources and systems. This might include, without limitation, the monitoring, 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.

Each Academy within the Trust 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 are advised to not use IT resources and communications systems for any matter that they wish to be kept private or confidential from the Academy in which they work.

From time to time, pupils will be monitored when using a computer. This will include student Internet activity and, where necessary, records of student Internet activity will be used in disciplinary procedures.

All internet access within the academy is monitored by the Internet Service Provider (ISP) and the Trust. Access to inappropriate content is flagged by automated systems and reported to safeguarding leads in the Trust for further investigation and action.

12. SECURITY

It is required that staff undertakes at least once a year GDPR and Cyber Security training provided by the school and IT Team. If the member of staff requires a knowledge refreshment, the training can be reviewed through the year as many times as needed.

Staff are advised to check their security profiles and privacy settings on the social networks that they use. If individuals are not clear about how to restrict access to their content, they should regard all content as publicly available and act accordingly.

In using social networking sites, staff are recommended to only post content that they would wish to be in the public domain. Even if content is subsequently removed from a site, it may remain available and accessible. Staff should consider not only how content could reflect on them, but also on their professionalism and the reputation of the Trust as their employer.

Even with privacy settings in place it is still possible that the personal details of staff may be accessed more broadly than the other networkers identified by them. Any reference to such information by pupils and/or their families, which a staff member deems to be inappropriate or is concerned about, should be reported to the Headteacher of the Academy they work at.

If a member of staff becomes aware that a pupil (or group of pupils) has made inappropriate/insulting/threatening comments about them, or other staff members, on a social networking site; then they must report this to the Headteacher so that the appropriate process can be followed.

Passwords and login details must be secure and not be written in a location visible or available to others.

For the MAT to be cyber security compliant, all systems managed by the MAT's IT Team are set to automatically install Operating System and Security updates as soon as the publisher releases them.

For Windows devices, **the users will receive default Windows notifications for actions that need to be completed for the update to be successful.** If the user hasn't completed the updates in the next 3 days since the update was released to the system, the device will automatically take charge and in some situations, with a 10 minute default warning message, it will restart the device.

!!! To avoid any unplanned restarts during important parts of the day, IT Team recommends that Windows devices should be shut down every night using the 'Update and Shut Down' option in the Start Menu.

Removable media devices

All connections from a device to another will be restricted except the wi-fi connectivity. Some examples of this will be AirDrop and Bluetooth, and others depending on technology.

Removable media devices include, but are not restricted to the following:

- CDs
- DVDs
- Optical Disks
- External Hard Drives
- USB Memory Sticks (also known as pen drives or flash drives)
- Media Card Readers
- Embedded Microchips (including Smart Cards and Mobile Phone SIM Cards)
- MP3 Players
- Digital Cameras
- Backup Cassettes
- Audio Tapes (including Dictaphones and Answering Machines)

This aims to ensure that the use of removable media devices is controlled in order to:

- Enable the correct data to be made available where it is required
- Reduce and mitigate risk
- Maintain the integrity of the data
- Prevent unintended or deliberate consequences to the stability of SFH

computer network

- Avoid contravention of any legislation, policies or good practice requirements
- Build confidence and trust in the data that is being shared between systems
- Maintain high standards of care in ensuring the security of Protected and Restricted information
- Prohibit the disclosure of information as may be necessary by law

At Excelsior Multi Academy Trust we do not allow the use of removable storage devices as transfer of data is facilitated through the Microsoft 365 cloud solution. The only exception will be when a school has not been migrated to the cloud where we will allow encrypted removable media to be used to transfer files. The migration to Microsoft 365 should be done as soon as possible followed by the block of all removable media to comply with this policy. All staff will be given a notice period, agreed with the HT of the school, through emails, to transfer all their files to the new cloud storage. After the notice has ended, if files are still on removable media, the user should open a ticket with the IT team as only IT team will be able to support in this matter.

IT Team, in some situations like installing new Operating System on a device or joining the device to the cloud Mobile Management solution, require use of USB memory sticks. These memory sticks will be used **only with the IT laptops and new devices and only transferring information deemed secure (Windows setup files, profiles to connect to the cloud...)**. This type of work will be carried out only in authorised locations. The security policy put in place across the MAT scans all files downloaded from the network or from the Internet. The security policy also forces Real-Time Protection to be ON and can't be turned off, enabling this feature to scan in real-time any file before it is accessed. Another setup allowing us to keep everyone safe is the daily antivirus quick scan at 3pm and weekly antivirus full scan which runs every Tuesday at 10am.

BYOD (bring your own device)

The purpose of this section is to establish the criteria of using personal owned devices (laptop, mobile phone, tablet) on school premises.

The MAT will not allow for your personal devices to be brought on site and to connect to the school network or systems. Copying information from the MAT's systems to your personal device is also prohibited and this should be done only on MAT provided devices.

For internet on your mobile phone, you must use your mobile data and you should never use the phone in the classroom or in the presence of pupils. The only exception is to authenticate to your Office365 account when MFA (Multi Factor Authentication) is present on that account and is requested by the computer. In this situation the phone should be put away immediately after authenticating was successful.

Cloud Storage

Cloud storage providers are applications that users access via the Internet. These services are contractually provided by companies such as Apple, Google, Microsoft, Amazon and others. They are accessible over the Internet through a variety of platforms (workstations, laptops, tablets, and smart phones).

Strictly no school data should be stored on any cloud service except the one provided by the school in Microsoft 365 (Office 365).

All school users have access to Microsoft One Drive and SharePoint Libraries through their Microsoft account provided by the school. Under no circumstances should school files / folders be saved on other cloud storage providers.

!!! It's every user's responsibility to act upon unauthorised users accessing drives that should not have access to, and they should notify the HT of the school and the IT Team straight away for further investigation.

When sharing information from personal OneDrive, regardless of how this is shared or to whom, users must enforce a time limit of no longer than 1 month (30 days). This is set under the 'Set expiration date' option.

Excelsior Multi Academy Trust provides a secure private cloud service that allows staff to access shared drives from outside of school. Some files and folders are restricted over the cloud to protect critical sensitive data. At all times we have systems in place monitoring each user's activity, this includes but not restricted to: email tracking, files download or modified, files moved or deleted.

13. LEGAL POSITION

Users should be aware that electronic text, such as e-mail, has the same status in law as the printed word. This means that e-mail communications can be potentially actionable in law in exactly the same way as the printed word for breaches of the relevant legislation such as the Data Protection Act or laws surrounding libel or defamation.

Copyright and intellectual property rights for online materials must also be respected.

The Trust may exercise its right to monitor the use of the school's computer systems, including access to web sites, the interception of e-mail and the

deletion of inappropriate materials where it believes unauthorised use of the school's computer system is or may be taking place, or the system is or may be used for criminal purposes or for storing unauthorised or unlawful text, imagery or sound.

The ICT department will be asked by SLT to check any student mobile phone that has been confiscated and/or social networking sites if they believe that illicit or criminal activity is taking place.

14. MOBILE PHONES

Personal mobile phones must not be used during working hours, in the classroom and during lessons unless approved by the Headteacher or in lessons by pupils, if a member of staff has sanctioned the device's use for learning purposes.

Using mobile devices to take photographs or videos of pupils without Headteacher's permission or staff without their knowledge or permission will be regarded as a serious misuse of a mobile device and is not permitted.

Posting videos or photographs, in school or online, of pupils without consent from parent/guardian will be regarded as a serious misuse of a mobile device and is not permitted.

Bullying by the use of text or multimedia messaging is not permitted, as are any other instances of inappropriate messaging or posts to social networking or blogging sites. The Trust is committed to ensuring the safety of all staff, pupils and visitors to our community. We will not condone bullying of any kind, including cyberbullying. Persons found guilty of committing cyberbullying will be dealt with in accordance with our Behaviour for Learning and Anti-bullying policies.

Victims and their families will always be advised by the Trust to contact their mobile phone provider, email provider and the police to report any such behaviour.

Safeguarding of our users is paramount however, in some situations, the IT Team and the Site Team will have to use a mobile phone in the classroom to rectify any issues that require 3rd party assistance. The use of mobile phones in classrooms should be questioned by any member of staff if unsure of the necessity of it and reported to the Headteacher if the user abuses this policy. At no given time should the IT or Site staff use the phone to take photos of pupils or members of staff and if there is a need for a photo to be taken it should be done only with the devices provided by the MAT.

15. USE OF DEVICES AND SCHOOL SYSTEMS FROM HOME (STAFF)

Please note that school devices are only the property of staff whilst they are employed at The Trust. You will be asked to return your laptop if you leave.

- All laptops will be password protected and encrypted

- Passwords must be changed in line with school policy, kept secure and changed regularly
- All devices must be covered on household insurance policies
- Devices will be audited by Technicians regularly for appropriate use
- Devices will be monitored for any inappropriate use all the time
- Staff must ensure that any access to the school data is protected by anti-virus and firewall software
- Under no circumstances is anyone other than the authorised employees to access the school systems
- Under no circumstances information that belongs to the school or MAT should be stored on a personal device

16. RECRUITMENT

Unless it is in relation to finding candidates (for example, if an individual has put his/her details on social media websites for the purpose of attracting prospective employers), the Trust will not, either directly or through a third party, conduct searches on applicants on social media. This is because conducting these searches during the selection process might lead to a presumption that an applicant's protected characteristics (for example, sexual orientation or religious beliefs) played a part in a recruitment decision.

17. REPORTING INCIDENTS

When reporting IT incidents regarding devices, subscriptions, applications or cyber risks, users are required to promptly notify the IT support team through the helpdesk system. This ensures that all issues are documented and addressed in a timely manner. Users should provide detailed information about the incident, including the nature of the problem, any error messages received, and the steps taken prior to encountering the issue. This helps the IT team diagnose and resolve the problem more efficiently. Additionally, users are encouraged to follow up on their reports if they do not receive a response within the expected timeframe. Maintaining clear and open communication with the IT support team is crucial for the swift resolution of incidents and the overall security and functionality of the IT infrastructure.

18. POLICY BREACHES

Staff found to be in breach of this policy may be subject to disciplinary action, in accordance with the Trust's Disciplinary Policy & Procedure with potential sanctions up to and including dismissal.

Information shared through social networking sites, even on private spaces, is subject to copyright, data protection, freedom of information, equality, safeguarding and other legislation.

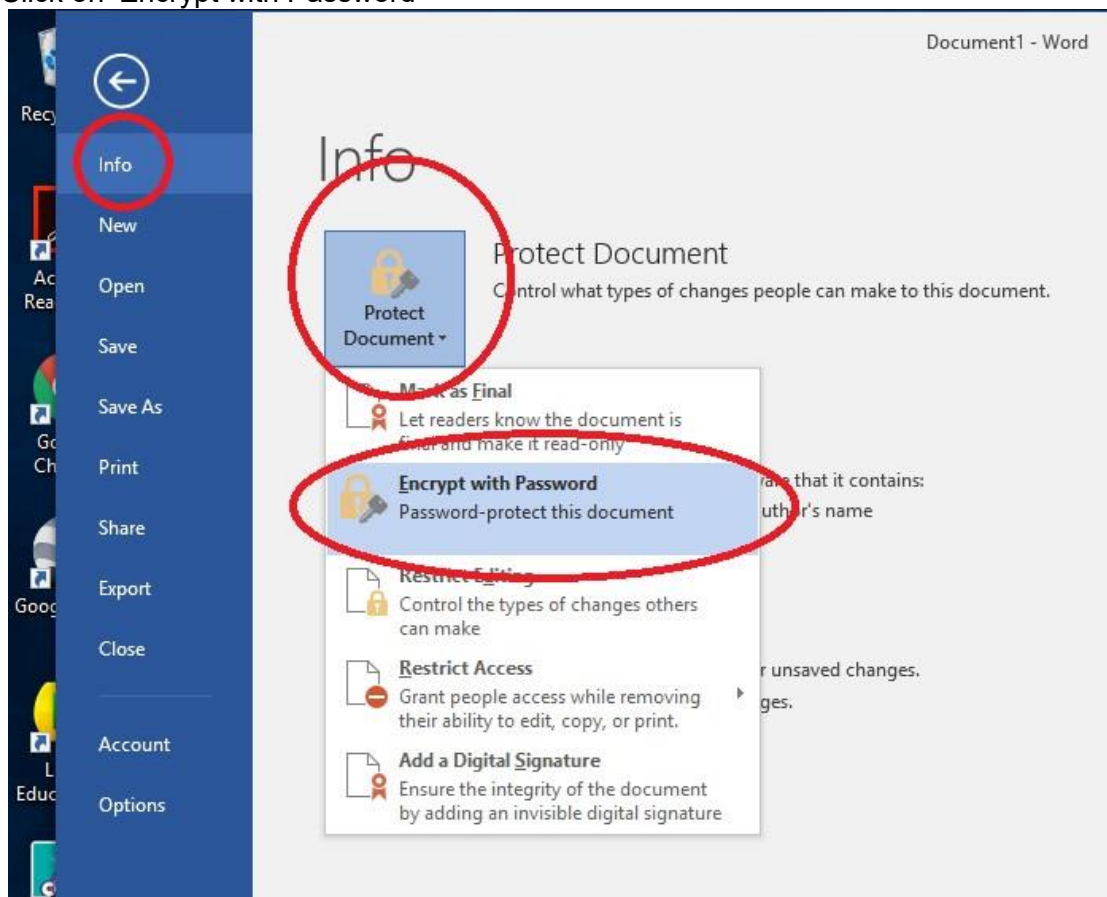
Where staff work in roles that are governed by professional bodies/professional codes of conduct; the professional rules relating to social networking applied to them may be more stringent than those within this Policy.

To support our staff, we have attached ANNEX 1 to ANNEX 3 on the next pages.

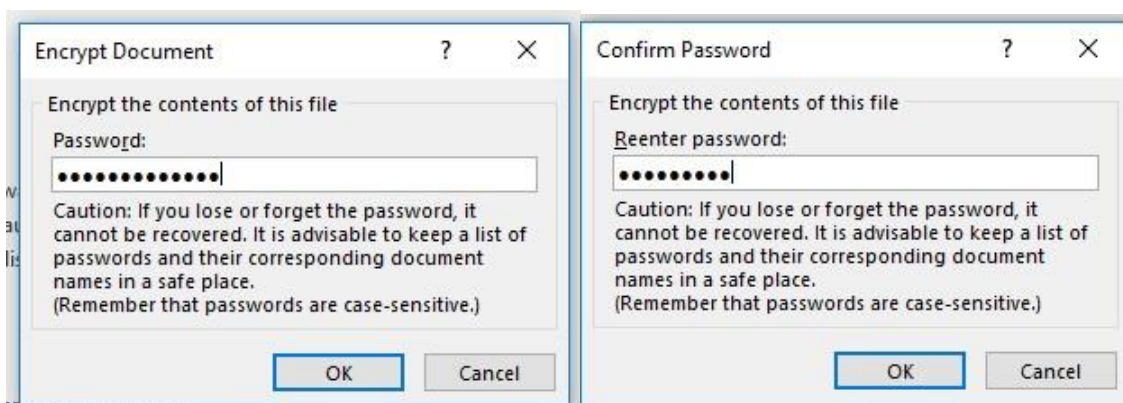
Annex 1

How to password protect a Word/Excel/PowerPoint document

After you finish editing the file press 'Save' and go to 'File' and 'Info'
You will see a tab called 'Protect Document', click on it
Click on 'Encrypt with Password'



A prompt to enter password will appear. Type in the password and then confirm the password.



Once done, you should see this:



When someone tries to open this document they will be prompted for a password



To remove the password, go to 'File/Info/Protect Document/Encrypt with Password' and in the password window just delete every character and press OK.

Procedures to follow when forming and remembering your password

1. Never reveal your password to anyone else or ask others for their password.
2. 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, DoB 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 'l' or '@' for 'A', '!' for 'i' etc. This will help to make your password much more difficult to guess. Remember that passwords are case-sensitive.
3. Users must utilise a complex password – random character and numbers in mixed case:
 - a. Password must meet complexity requirements:
 - i. Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
 - ii. Be at least 6 (six) characters in length
 - iii. Contain characters from three of the following four categories:
 - English uppercase characters (A through Z)
 - English lowercase characters (a through z)
 - Base 10 digits (0 through 9)
 - Non-alphabetic characters (for example, !, \$, #, %)
4. If you forget your password, please request that it be reset by your IT coordinator
5. If you believe that a student or other staff may have discovered your password, then change it immediately
6. Never use the feature 'Remember password'
7. You must change the passwords every time the system will prompt you. Do not use variations of the old password.
8. Never leave your computer unattended while using any personal data – if called away you should lock the workstation – this will normally require a password to reopen.
9. If you leave your computer unattended, particularly in a classroom, either log out or lock it by using the CTRL-ALT-Delete keys and then choosing "Lock " or by pressing the Windows key + L key. Once this is done, you will need to re-enter your password to gain access to the computer.
10. Never allow another person to login to any system with your login ID and password.
11. Auditing measures in place could result in you being responsible for the actions of another person. This is particularly risky in a situation where you as an adult allow a child to access materials under your login.
12. Never write your password down and leave it out for others to find.

Password Guide Do's & Don'ts

DO 	DON'T 
KEEP YOUR PASSWORD A SECRET	TELL ANYONE YOUR PASSWORD
USE CAPITALS, NUMBERS AND SYMBOLS	USE NAMES OR BIRTHDATES
MAKE SURE YOUR PASSWORD IS LONGER THAN EIGHT CHARACTERS	USE SIMPLE PASSWORDS SUCH AS 'Qwerty123'
USE TWO-STEP VERIFICATION WHERE POSSIBLE	USE THE SAME PASSWORD ACROSS ACCOUNTS
	

Annex 3

GDPR compliant record sheet of personal/sensitive information being taken off site.

Date data being taken out	Person requesting to take data off site	Reason for taking data off site	Time out	Time returned	Signature