Executive Principal: Sir J A Townsley BA (Hons) NPQH

Chair of the Board: Mr T Elliott

E-safety and online Policy

Designated Teacher:	Trust Director of IT
Reviewed by:	Governors Policy Committee
Review Cycle:	5 Years

Fountain Street, Morley, Leeds LS27 0PD
T 0113 253 2952 **F** 0113 253 1483
E info@morley.leeds.sch.uk
W www.morley.leeds.sch.uk

TGAT E Safety Policy

1. INTRODUCTION

1.1 The Trust recognises that ICT (Information and Communication Technology), the internet, and social networking can be important tools for aiding teaching and learning, providing opportunities for research and investigation and create a forum for the communication of ideas. Technology enriches the curriculum, enhances the learning experience of students and supports creativity and independent thinking.

1.2 The use of ICT to interact socially and share ideas can benefit staff, students and parents/carers across the Trust; however, it is important that the use of the internet, tablets, e-readers, gaming systems and mobile phones is seen as a significant responsibility for students, staff and parents/carers that must be used appropriately.

1.3 It is essential that all staff, students and parents/carers from each Academy are alert to e-safety and the possible risks when using the internet and chat rooms, social networking, gaming and mobile phones with internet access. It is also important that staff, students and parents/carers are aware of the importance of responsible conduct online.

1.4 We know that some adults and young people will misuse mobile phones, the internet, chat rooms and social networks to harm children and young people. The harm might range from sending abusive texts and emails, to harassment and stalking behaviour and coercing children and young people to engage in sexually harmful conversations or actions online; such as webcam filming, sending explicit photographs, or arranging face-to-face meetings. This can also lead to blackmail, sharing of inappropriate images, CSE (Child Sexual Exploitation) and sexual abuse.

1.5 Staff members at each Academy have a responsibility in accordance with 'Keeping Children Safe in Education' (DfE, 2015) to safeguard students and report abuse immediately to designated staff members, as per the Trust's Child Protection Policy. Every member of staff will attend child protection training which outlines forms of abuse, and includes the indicators and signs of CSE.

1.6 All staff members have a 'duty of care' to ensure that students are educated about e-safety, know how to reduce risk of harm and stay safe, are able to report abuse and know who to talk to about any concerns around the use of this technology. There is also a duty to ensure that staff conduct does not bring into question their suitability to work with students.

1.7 When used in the correct manner this technology can give students, staff and parents/carers many opportunities for personal development and there needs to be a balance between controlling access to the internet and technology and allowing students the freedom to explore and use these tools to their full potential.

1.8 The Trust will appoint an e-safety officer who will ensure the development of an e-safety policy, oversee the procedures outlined in the policy and provide advice for staff and students about e-safety.

1.9 Each Academy will nominate an e-safety officer who will be a member of the Senior Leadership Team and a Governor with responsibility for e-safety to implement the e-safety policy and ensure it is disseminated to staff.

2. AIMS OF E-SAFETY POLICY

2.1 This policy aims to outline procedures for the use of ICT and technology by staff and students across the Trust and at each Academy.

2.2 The policy will define the code of conduct for staff when online and when using related technologies, and provide e-safety guidelines.

2.3 The policy aims to raise awareness of good e-safety practice focused upon the value and benefits of using ICT and related technologies, whilst being mindful of the possible risks and dangers involved.

2.4 This policy is available on each Academy website for access by parents/carers, staff and students.

2.5 Throughout this policy children and young people are referenced as students. For the purpose of safeguarding and child protection. The term students include all children, young people and young adults at risk who professionals may come into contact with, as part of their role.

3. PROFESSIONAL EXPECTATIONS

3.1 The use of computer systems without permission or for purposes not agreed could constitute a criminal offence under the Computer Misuse Act 1990.

3.2 Staff members at each Academy are adults and as such should act responsibly and with an awareness of the consequences of their actions. Staff members must act with the best interests of students at all times.

3.3 Staff who are provided with a laptop or tablet by the Academy must use this only for academic purposes, these remain the property of the Academy and open to scrutiny by Senior Leaders.

3.4 All staff members are responsible for their personal use of social media, networks and electronic device and are expected to ensure that any use of such technologies does not breach the Trust's Safer Working Practice or undermine the reputation of the Academy and Trust.

3.5 Trust staff are personally responsible for the security and privacy settings when using social media and networks and failing to ensure that privacy settings are secure could lead to a disciplinary process if the content breaches professional expectations.

3.6 Trust staff must ensure that their use of ICT and social media is professional at all times, even if this is outside of the Academy day, and that behaviour which breaches the Trust's code of conduct could lead to disciplinary action.

3.7 All contact made with students must be made through appropriate channels, such as teaching and learning blogs, and should be made within clear and transparent professional boundaries and only made with regard to matters regarding the Academy.

3.8 Trust staff must not give out personal details, such as telephone numbers, email addresses, social media identities to students, ex–students or parents/carers of students. Any contact made with ex–students should not be made if they are under the age of 18, are currently a student at the Academy or in full time education. Great caution should be advised with regards to any contact with any ex – students and staff members must use their personal judgement and be mindful of their professional standing. Any member of staff found to be in contact with students, ex – students and parents/carers in this way, without consent from the Principal may be subject to disciplinary action.

3.9 Trust staff should be aware that when giving information or reprimanding students they should do it in a tone or manner which they would be happy for a parent to witness. Please be aware that due to the development of smart phone technologies recording of dialogue between staff and students is an increasing possibility.

3.10 Safe and professional behaviour of Trust staff online will be discussed at staff induction training. This relates to the use of social networking sites outside of the working environment. As a Trust employee it is important to be aware that posting information or views about the Trust or Academy cannot be isolated from your working life. Comments about the Trust or Academy, students, parents/carers or colleagues can bring the Trust and Academy into disrepute and make both the Academy and the employee liable to legal action.

3.11 **Appropriate computer usage**

3.11.1 Staff members are expected to use computers in lessons only for teaching and learning and not for other Academy work.

3.11.2 Trust staff should ensure that students are unable to access activities and information on the computers that is not relevant to teaching and learning and the lesson.

3.11.3 Staff should log off or lock their computer when not in use to protect confidential and personal information.

3.11.4 Only IT Technicians should move computer equipment, unplug cables or remove screws or covers from equipment and upload/download or copy programs and change, or attempt to change the configuration of any computer.

3.11.5 Students should not use computers in classrooms without permission or without a member of staff being present, specifically at non-contact times to ensure that staff members are able to supervise online access and secure equipment.

3.11.6 Any misuse or damage to computers in classrooms should be reported to technicians immediately.

3.11.7 Staff may be liable to pay for any damage caused by themselves to Academy equipment intentionally or accidently. Each circumstance will be dealt with individually by the Principal.

3.12 **Social media and networks**

3.12.1 Staff members should not be in contact with students, ex- students in full time education or parents/carers of students using social media and networking, unless prior permission has been given by the Principal or you have known them previously on a personal level before they started at the Academy.

3.12.2 Students should not be added as friends and staff must not respond to friend requests. If a member of staff suspects that an existing friend is a student or a student is using another name to befriend the member of staff the friendship should be ended and this should be reported to the Principal.

3.12.3 If a member of staff coincidently has a contact established with an ex-student, parent/carer or student the member of staff must use their judgement and regulate this contact. If a student, ex-student or parent/carer persistently attempts to befriend a member of staff this should be disclosed to the Principal.

3.12.4 The use of personal social networking activity is at the discretion of the individual, however the professional responsibilities of the individual need to be considered in all postings on this sites.

3.12.5 It is important to ensure that your personal information is secure and that high strength passwords are used and that profile settings are restricted. It is advisable to log out of social networking sites when not in use as a security precaution.

3.12.6 Staff must be aware of how to set privacy settings on their profile (refer to Annex A) and be mindful that some social networking sites revert to default settings when an update is made to their service. Staff should be vigilant to any changes in their profile privacy settings.

3.12.7 Professionals should consider what information they use for their profile, for example the photograph and the amount of personal information that is displayed. Profiles should not identify your employer or place of work.

3.12.8 Staff should not publish their Academy email address on a personal social networking site, or use this address as part of your login/registration on a personal site.

3.12.9 All postings on social media and networks should be considered to be in the public domain so staff members should consider this when making decisions about the content of social media activity.

3.12.10 Any material which is posted on social media and networks which is considered to bring the Trust and Academy into disrepute or is considered to put students or staff at risk of harm will be dealt with under the Trust's Disciplinary Procedure and follow the Allegations Management Policy.

3.12.11 Staff members should not make reference online to any students, parents/carers, colleagues or to any work related issue. This also includes posting photographs or videos online which identify your place of work, or any students and parents/carers.

3.12.12 While access to social media sites through the Academy network is blocked to employees, accessing the internet through mobile phones and other mobile devices is prohibited during working hours. Staff members should never use Academy networks or equipment to access or update a social media site.

3.13 **Facebook and Twitter advice**

3.13.1 Facebook and Twitter are media that can have enabled families and friends to stay in contact and have lessened geographical divides, it is important, however that this media is used appropriately. To ensure that staff are safe and protected as professionals:

- Keep your profile picture post modest. Remember students can still search for you and see your picture without being your friend.
- Create your photo albums with privacy settings so 'only your friends' can see them.
- Reject all friend requests from students. You do not need to report this unless it becomes a recurring problem. People are not notified when you reject their friend request.
- Use the Facebook/Twitter privacy settings to limit who can see your full profile. Set it so that only friends can see everything like your pictures, your wall, and your personal and contact information.
- Use limited public information about yourself on your profile. For example address, email, date of birth, contact telephone numbers do not need to be shown to everyone, they can be privately messaged if needed.
- Do not use your Academy email address as your email contact.
- Do report any threats of violence or other inappropriate posts/images to Facebook or to the relevant authorities, such as CEOP (Child Exploitation and Online Protection centre) or the police.
- Customise your privacy settings. Limit what people can see when you 'poke' or message them before you have added them as a friend. The default setting allows people who are not friends whom you 'poke' or message to see your entire profile.
- Don't ever announce on your wall if you're going away. Many cases of burglaries are supported through the use of these disclosures on Facebook and Twitter.

3.14 **The use of mobile phones and personal devices**

3.14.1 Under no circumstances should staff use their own personal devices to contact students or parents/carers either in or out of Academy time.

3.14.2 Staff are not permitted to take photos or videos of students. If photos or videos are being taken as part of the Academy curriculum or for a professional capacity the Academy equipment will be used. Any device which takes images, videos, moving images should not be used during working time as this breaches safeguarding and child protection responsibilities.

3.14.3 The use of personal equipment in the Academy can only be authorised by the Principal or Senior Leadership Team in order to comply with safer working practice guidance, data protection and Trust policies.

3.14.4 Any breach of the Trust E-safety and Online Policy may result in disciplinary action against that member of staff. More information on this can be found in the Child Protection Policy and Allegations Management Policy.

3.15 Inappropriate material

3.15.1 In law there is a distinct difference between material that is inappropriate and that which is illegal, however accessing of inappropriate material is a significant concern with regards to safeguarding. Staff should be aware that the accessing of illegal material will lead to a case investigation, allegations management procedures, a possible criminal investigation, prosecution and barring, even if there is no criminal prosecution.

3.16 Illegal material

3.16.1 It is illegal to make, possess or distribute indecent images of a person under the age of 18 and viewing these images online may constitute possession even if they are not saved. Accessing indecent images of children or students on the internet or making, storing or distributing such images of students or children is illegal and if proven could lead to criminal investigation and the individual being barred from working with students.

3.17 Materials which incite hate, harm or harassment

3.17.1 There are a range of offences in relation to incitement of hatred on the basis of ethnicity, gender, sexual orientation, gender identity religion and beliefs and offences concerning harassment and threatening behaviour which include cyber bullying, whether this is carried out on a mobile phone, social networking or through email. It is an offence in law to send indecent, offensive harassing or threatening messages which cause the recipient distress. Hate crime is a matter for the police and they must be called if a student or member of staff is victim to a hate crime.

3.14 Professionally appropriate material

3.14.1 Trust staff should not use any equipment belonging to the Academy to access adult pornography and equipment with links and images on personal equipment should not be brought into the Academy.

3.14.2 Trust staff should be aware that actions outside of the Academy which are not professionally appropriate and which fundamentally breach the staff code of conduct could result in disciplinary action. Examples of inappropriate materials and actions which breach trust and confidence in professionals are:

- Posting offensive, harassing threatening or bullying comments about colleagues on social networking sites
- Making derogatory comments about students, colleagues, the Academy or Trust
- Posting unprofessional comments about one's profession
- Making inappropriate statements or using offensive or hate based language.

3.15 Confidentiality and Data

3.15.1 Members of staff have access to confidential information about students, other staff and parents/carers in order to undertake their daily duties, this may sometimes include highly sensitive information. This information must not be shared outside of the Academy or with external parties unless a student is at risk of harm or significant harm or there is an agreed multi-agency plan around a family and student.

3.15.2 Confidential information should only be stored on Academy systems and email should never be used to transfer sensitive and confidential information. In such cases, sensitive and confidential information should only be shared using mail express or other secure methods of communication.

3.16 Cyberbullying

3.16.1 Cyberbullying, bullying, harassment, defamatory comments, offensive correspondence and hate incidents within and outside the Academy will not be tolerated and any member of staff found to be behaving in this manner towards colleagues will be dealt with in accordance with the Bullying and Harassment Policy and in specific circumstances will be considered as a criminal offence.

3.16.2 If any member of staff is a victim of this behaviour they must follow the Whistleblowing Policy and report this behaviour as soon as possible to their line manager or Principal. The victim will be offered support and this will be fully investigated and the Bullying and Harassment Policy followed, a referral may be made to the appropriate authorities if deemed appropriate.

3.17 Academy email accounts, etiquette and appropriate use

3.17.1 Staff must only use their own Trust account internet and email password, and not share this password.

3.17.2 Email etiquette should be observed and emails should be written carefully and politely, the tone of an email should be considered before sending. Emails should be sent to specific member/s of staff and not just a general distribution list, unless applicable and should have a specific title related to the content. Content of emails should be simplified into simple bullet points as much as possible and the 'High importance' feature should be used only if a matter is urgent. Staff should try and respond to email requests as efficiently as possible, however, where possible staff are encouraged to have more face-to-face communication with colleagues.

3.17.3 To ensure that we create a professional environment the sending of anonymous messages and chain letters is not allowed.

3.17.4 If an email is received with an attachment it must not be opened unless the sender is known. If in doubt, check with the IT Technicians.

3.17.5 All emails that need to be actioned by the following working day should be sent no later than 4.00pm of that day, unless as a matter of urgency.

3.17.6 In order to manage data all emails should be deleted when read if not needed at a later date. Staff should try and use the calendar or flagging system in their emails and delete their inbox, deleted and sent items regularly.

4. POLICY AND GUIDANCE FOR THE SAFE USE OF STUDENT PHOTOGRAPHS

4.1 Photographs, images of students work and recorded images are part of daily Academy life and enhance the learning experience and environment for our students, parents/carers and staff members. They are used to showcase the talents and work of our students, express our pride for our Academy and celebrate the talents of the student body. We therefore acknowledge the importance of having safety precautions in place to prevent the misuse of such material.

4.2 Under the Data Protection Act 1998 images of students and staff will not be displayed in public, either in print or online, without parental permission. On admission to the Academy parents/carers will be asked to sign a photography consent form. The Academy does this so as to prevent repeatedly asking parents/carers for permission over the academic year.

4.3 Images of students must not be displayed or distributed, for example in a newsletter or website, without parental permission.

4.4 Using photographs of students

4.4.1 Photographs and video images must be created with Academy equipment only. No members of staff should use personal devices to record or store images of students.

4.4.2 It is important that published images do not identify students or put them at risk of being identified. The Academy is careful to ensure that images published on the Academy website cannot be reused or manipulated through watermarking and browser restrictions. Only images created by or for the Academy will be used in public and students may not be approached or photographed while in the Academy or doing Academy activities without the Academy's permission.

4.4.3 Electronic and paper images of students will be stored securely and the names of stored photographic files will not identify the student.

4.4.4 Images will be carefully chosen to ensure that they do not pose a risk of misuse. This includes ensuring that students are appropriately dressed. Photographs of activities which may pose a greater risk of potential misuse (for example, swimming activities), will focus more on the sport than the students (i.e. a student in a swimming pool, rather than standing by the side in a swimsuit).

4.4.5 When images are used for public documents, including in newspapers, full names will not be published alongside images of the student. Groups may be referred to collectively by year group or form name.

4.4.6 Events recorded by family members of the students such as Academy plays or sports days must be for personal use and only at the discretion of the Academy.

4.4.7 Students are encouraged to tell a member of staff if they are concerned or uncomfortable with any photographs that are taken of them or they are being asked to participate in.

4.4.8 Any photographers that are commissioned by the Academy will be fully briefed on appropriateness in terms of content and behaviour, will wear identification at all times, and will not have unsupervised access to the students. For more information on safeguarding in the Academy please refer to our Trust Child Protection Policy.

4.4.9 Child Protection Designated Officers are aware of students who need protection from their image being used and will ensure that staff members are made aware of students who cannot have their image published in any form.

4.5 Complaints of misuse of photographs or video

4.5.1 Parents/carers should follow the Trust Complaints Policy if they have a concern or complaint regarding the misuse of Academy photographs. Any issues or sanctions will be dealt with in line with the Trust Child Protection Policy and Positive Discipline Policies.

5. CONSEQUENCES OF INAPPROPRIATE ACTION BY STAFF MEMBERS

5.1 The Trust may exercise the right to monitor the use of the Academy computer systems, including access to websites, the interception of email and the deletion of inappropriate materials, without the consent of the staff member.

6. TEACHING AND LEARNING THROUGH ICT

6.1 E-safety is integrated into the Academy curriculum in every circumstance where the internet or technology are being used, and during PSHCEE (Personal, Social, Health, Citizenship and Economic Education) lessons where personal wellbeing is being taught, please see the Trust's PSHCEE and SRE (Sexual Health and Relationships) Policies for further details.

6.2 Students will be made aware about the possible risks and dangers that they might encounter when using ICT, the internet, mobile phones, gaming stations and personal devices through ICT lessons, implicitly throughout the curriculum and in PSHCEE. This will include understanding how photographs can be manipulated, the importance of keeping personal information private, information about safe social networking and chat rooms, ownership of personal images, sexting and healthy relationships, awareness of CSE and the implications of inappropriate posts and images on career progression and employment, as well as many other topics.

6.3 The internet is used in each Academy to raise educational standards, promote student achievement, support the professional standards of the work of staff members and to enhance the Academy's management functions. It is the responsibility of every staff member to equip students with the necessary ICT skills, transferable knowledge and awareness to enable them to make outstanding progress, fulfil their potential and secure further and higher education, apprenticeships and/or employment.

6.4 Students will have access to ICT and e-safety information as part of their ICT curriculum, and/or via access to the ICT where they can access a number of teaching and learning resources. To enable students to expand their horizons they have unlimited access to worldwide educational resources and institutions such as art galleries, museums and libraries and can contact schools in other countries resulting in cultural exchanges between students all over the world.

6.5 Teaching and Learning is enriched by access to subject experts, role models, inspirational people and organisations and an enhanced curriculum; this includes;

- interactive learning tools
- access to case studies, videos and interactive media to enhance understanding, collaborative activities, locally, nationally and globally
- self-evaluation
- feedback and assessment
- updates on current affairs.

6.6 ICT can be used to give students the freedom to be creative and the opportunity to explore the world and its differing cultures from within a classroom. It can be used as a tool for social inclusion, in class and online and to provide individualised access to learning.

6.7 For staff ICT can aid professional development through access to national developments, educational materials and examples of effective curriculum practice and classroom strategies. It can allow professionals to access professional support through networks and associations. It is a communication tool which gives professionals the ability to mark and assess student work and provide immediate feedback to students and parents/carers. It is also an administrative instrument used for class management, attendance records, schedule, and assessment tracking.

6.8 Engagement with parents/carers is important and integral to the work of staff and ICT gives parents/carers access to the Academy parent/carer website pages with a wide variety of educational resources to help support students with homework and to aid learning from home.

6.9 **Learning to evaluate internet content**

6.9.1 There is a multitude of information available online and it is important that students learn how to evaluate internet content for accuracy and intent. Students are taught

to become digitally literate across the whole curriculum and are encouraged to be critically aware of materials they read, and how to validate information before accepting it as accurate. Students will be taught to understand the bias of web authors, separate fact from fiction and practice etiquette on the internet, emails and social media. Students learn how to use age-appropriate tools to search for information online, how to acknowledge the source of information used and to respect copyright.

6.9.2 Plagiarism is against the law and the Academy will take any intentional acts of plagiarism seriously. Students who are found to have plagiarised will be disciplined in accordance with the Trust's Positive Discipline Policies. If plagiary has occurred during an exam or a piece of coursework the student may be prohibited from completing that exam.

6.9.3 The Academy will also take steps to filter internet content to ensure that it is appropriate to the age and maturity of students. If staff or students discover unsuitable sites then the URL must be reported to the Academy E-safety Officer and IT Technicians.

6.9.4 Any material found by members of the Academy that is believed to be unlawful will be reported to the appropriate agencies. Regular software and broadband checks will take place to ensure that filtering services are working effectively.

7. MANAGING VIDEO CONFERENCING AND WEBCAM USE

7.1 Video conferencing should use the Trust portal rather than the internet to ensure quality of service and security. Students should have permission from the member of staff before making or answering video conference calls.

8. SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

8.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programmes and Twitter. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by a dangerous person.

8.2 It is important that we educate students so that they can make their own informed decisions and take responsibility for their conduct online. Staff and students are not allowed to access non–academic social media sites within the Academy.

8.3 Social media sites have many benefits for both personal use and professional learning; however, both staff and students should be aware of how they present themselves online. Students are taught through the ICT curriculum and PSHCEE about the risks and responsibility of uploading personal information and possible long term implications of this information being in the public domain.

8.4 Students are educated on the dangers of social networking sites and how to use them in safe and productive ways, and are all made fully aware of the Academy's Code of Conduct regarding the use of ICT and technologies and behaviour online.

8.5 Any sites that are to be used in class will be risk-assessed by the teacher prior to the lesson to ensure that the site is age-appropriate and safe for use.

8.6 Official Academy blogs created by staff or students, year groups or Academy clubs will be password-protected and will be incorporated on the Academy website with the prior approval of the Principal and with permission from a member of staff.

8.7 Staff and students are encouraged not to publish specific and detailed private thoughts, especially those that might be considered personal, sensitive, hurtful, harmful, hateful or defamatory. The Trust expects all staff and students to remember that they are representing their Academy and the Trust at all times and must act appropriately.

9. EQUAL OPPORTUNITIES

9.1 The Trust believes that it is essential that everyone can have access to ICT and that opportunities are provided for all students, regardless of ethnicity, beliefs, values, religion, gender, culture, physical and mental difficulty.

9.2 This is underpinned by the requirements set out in the Equalities Act 2010.

10. SPECIAL EDUCATIONAL NEEDS AND DISABILITIES (SEND)

10.1 ICT can be a positive tool for students with SEND and access to the internet and ICT is a vital link for communication with the outside world and other students, which can allow every student to have access to information, communicate with others and develop ideas and research independently.

11. MONITORING

11.1 The Trust will take any issues identified by staff, students and parents/carers, regarding any breach of social media sites seriously and this will be investigated and dealt with by the Senior Leadership Team and Principal as set out in the Allegations Management Policy. If any staff member feels they need any statement clarified, the E-safety Officer, Network Manager or Partnership Director of IT will be happy to explain in more detail.

12. MOBILE PHONES AND PERSONAL DEVICES

12.1 While mobile phones and personal communication devices are commonplace in today's society, their use and the responsibility for using them should not be taken lightly. There are issues surrounding the use of mobile phones to video and take photographs of students and staff members for use in Cyberbullying and devices with integrated cameras, can lead to child protection, bullying and data protection issues. Mobile phones can also be used by students to access inappropriate internet material. If taken into the Academy they can be a distraction in the classroom and are valuable items that could be stolen, damaged, or lost.

12.2 Each Academy in accordance with the Trust's Positive Discipline Policies will take measures to ensure that mobile phones are used responsibly.

12.3 The Trust will not tolerate cyberbullying against either students or staff. Sending inappropriate, suggestive or abusive messages is forbidden and anyone who is found to have sent a message of such content will be disciplined. For more information on the Academy's disciplinary sanctions read the Trust's Positive Discipline Policies.

12.4 Images or files should not be sent between mobile phones in the Academy and mobile phones can be confiscated by a member of staff, and the device can be searched by a member of the Senior Leadership Team if there is reason to believe that there may be evidence of harmful or inappropriate use on the device.

12.5 Mobile phones must be switched off and secured in bags whilst on Academy premises.

12.6 Any student who brings a mobile phone or personal device into the Academy is agreeing that they are responsible for its safety. The Academy will not take responsibility for personal devices that have been lost, stolen, or damaged.

12.7 Students who breach the Trust policy relating to the use of personal devices will be disciplined in line with the Trust's Positive Discipline Policies. Their mobile phone may be confiscated.

12.8 Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms with them. If a student is found with a mobile phone in their possession it will be confiscated. The breach of rules will be reported to the appropriate examining body and may result in the student being prohibited from taking that exam.

13. MANAGING INFORMATION SYSTEMS

13.1 The Partnership Director of IT is responsible for reviewing and managing the security of the computers and internet networks along with the Network Managers and IT technicians. The Trust takes the protection of Academy data seriously and Academy networks are protected, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the Academy information systems and users will be reviewed regularly by the Partnership Director of IT and Network Managers and virus protection software will be updated regularly.

13.2 Some of the safeguards that the each Academy takes to secure computer systems are ensuring that all personal data sent over the internet or taken off site is encrypted, making sure that unapproved software cannot be downloaded to any Academy computer checking files held on the each Academy network for viruses.

14. EMAILS

14.1 Students should be aware that Academy email accounts should only be used for academy-related matters. Students and Parents should only be contacted via an

approved academy account. The academy has the right to monitor emails and their content, but will only do so with good reason.

15. CYBER-BULLYING

15.1 Cyberbullying is defined as bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as mobile phones, computers, and tablets as well as communication tools including social media sites, text messages, chat, and websites. Examples of cyberbullying include mean text messages or emails, rumors sent by email or posted on social networking sites, and distributing embarrassing pictures, videos, websites, or fake profiles.

15.2 Cyber bullying by students and staff will not be tolerated and will be treated as seriously as any other type of bullying. Information about specific strategies or programmes in place to prevent and tackle bullying can be found in the Trust's Positive Discipline Policies. All students at each Academy are aware of their rights and responsibilities with regards to bullying.

15.3 If a member of staff is aware of a bullying incident they must take this seriously, act as quickly as possible to establish the facts and report the incident to the appropriate member of staff who leads behaviour or safeguarding, such as an Assistant Principal, Head of Year, Inclusion Managers/Leaders, Head of Alliance, Designated Lead Child Protection Officer. These members of staff will investigate the matter fully, provide support for the victim, try to act restoratively and apply sanctions when necessary.

15.4 If a sanction is used, it will correlate to the seriousness of the incident and the 'bully' will be told why it is being used. The student will be asked to remove any harmful or inappropriate content that has been published, and the service provider may be contacted to do this if they refuse or are unable to remove it. The student may have their internet access suspended.

15.5 Any allegations of cyberbullying will be managed in accordance with the Trust's Anti-bullying and Hate Incident Policy and Positive Discipline Policies.

16. PUBLISHED CONTENT AND THE ACADEMY WEBSITE

16.1 Each Academy website is a tool for communicating the Trust and Academy ethos, academic pride and practice to the wider community. It is also a valuable resource for parents/carers, students, and staff for keeping up-to-date with Academy news and events, celebrating whole-Academy and individual student achievement, personal achievements, and promoting Academy projects, events and extra-curricular activities.

16.2 The website is in the public domain, and can be viewed by anybody online. Any information published on the website will be carefully considered in terms of safety for the Academy students and staff, copyrights and privacy policies. No personal information about students or staff will be published, and details for contacting the Academy will be for the Academy reception or office only

17. MANAGING EMERGING TECHNOLOGIES

17.1 Technology is progressing rapidly and new technologies are emerging all the time. Each Academy will risk-assess any new technologies before they are allowed in the Academy, and will consider their educational benefit. The Trust keeps up-to-date with new technologies and is prepared to quickly develop appropriate strategies for dealing with new technological developments.

18. PROTECTING PERSONAL DATA

18.1 The Trust believes that protecting the privacy of our staff, students and parents/carers and regulating their safety through data management, control and evaluation is vital to each Academy and to individual progress.

18.2 Each Academy collects personal data from students, parents/carers, and staff and processes it in order to support teaching and learning, monitor and report on student and teacher progress, and strengthen our pastoral provision.

18.3 Each Academy takes responsibility for ensuring that any data collected is used correctly and only as is necessary, and the Academy will keep parents/carers fully informed of how the data is collected, what is collected, and how it is used.

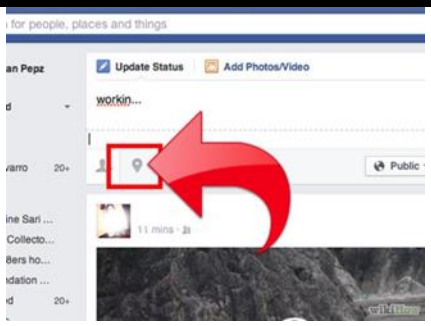
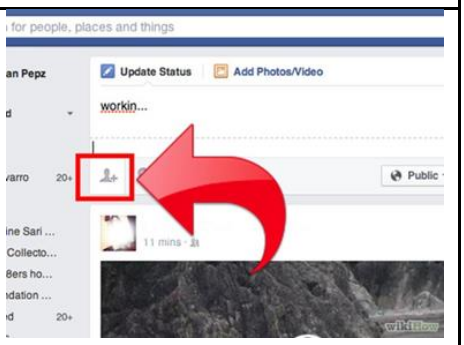
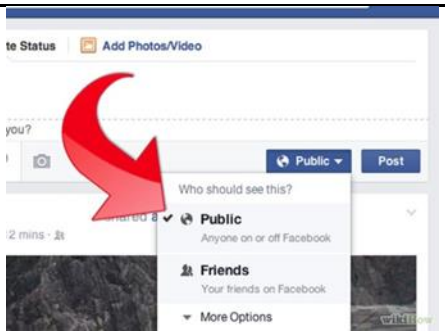
18.4 National Curriculum results, attendance, assessment data, registration records, SEND data, and any relevant medical information are examples of the type of data that the Academy will capture. Through effective data management we can monitor a range of provisions and evaluate the wellbeing and academic progression of students to ensure that they receive an outstanding education and to respond to the changing needs of students.

18.5 In line with the Data Protection Act 1998 and the Trust's Data Protection Policy, we will follow the principles of good practice when processing data. Each Academy will ensure that data is fairly and lawfully processed and only for limited purposes. The Academy will ensure that all data processed is adequate, relevant, accurate and not excessive. Data will only be kept for the period of time that is necessary. It will be processed in accordance with the data subject's rights and will always be secure and not transferred to other countries without adequate protection.

18.6 There may be circumstances where the Academy is required either by law or in the best interests of our students or staff to pass information onto external authorities; for example, our Local Authority, Ofsted, or the Department of Health. These authorities are up-to-date with data protection law and have their own policies relating to the protection of any data that they receive or collect.

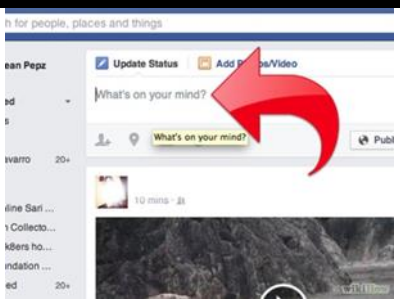
Annex A – How to Manage Facebook Privacy Options

Every so often, Facebook revamps their privacy settings to make them more user-friendly. Among the most recent new features are better control of your news feed, the ability to view your profile as another user, and a simplified privacy page. Need to navigate your privacy settings? With just a few tips, the new set-up will seem completely natural. Luckily, the new privacy settings are far more intuitive than before.

Method 1 of 4: Managing Status Updates	
1. Type your desired status into the newsfeed bar.	
2. Click the button on the bottom left to tag people with you. Type their names into the box that says "Who are you with?"	
3. Decide who can see the update. Before you click Post, click the drop down box just to the left of it. You can choose to set the status visible to the public, just your friends, or a custom set of people. • To make your updates available to friends of friends, click Custom, then select Friends of Friends on the drop menu. • To set your status visible to only a certain set of people, click "Custom." Then, choose an option from the drop down menu. To set it visible to one or two people, choose "specific people" and then type the names of the people to whom you would like to grant permission. • You can also choose to hide the update from one or two people by typing their name in the "hide this from" section of the custom settings.	

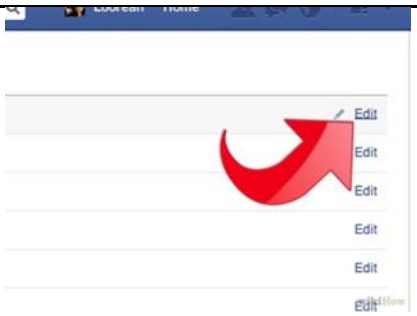
Method 2 of 4: Managing Profile Info

1. Access the "Edit Profile" page. This can be done by clicking the "Info" tab of your profile, and then hitting edit in the right corner (see picture). It can also be accessed by clicking "Edit My Profile" under your name on the home page.



2. Choose who can see what information. Beside each of piece information, you will see a drop down menu. You can decide which groups of people will see which information by clicking the menu and selecting the desired option

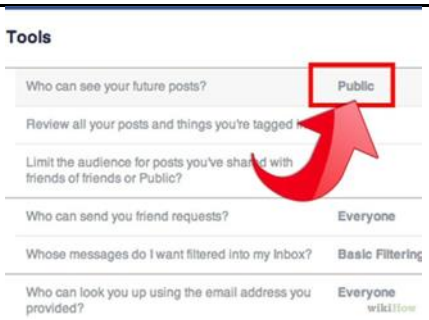
- This can differ for each post. For example, you can set your work place visible to the public, but only allow your friends to see where you went to college.
- Toggle between different sections of your profile by clicking the options on the left hand side of the page.



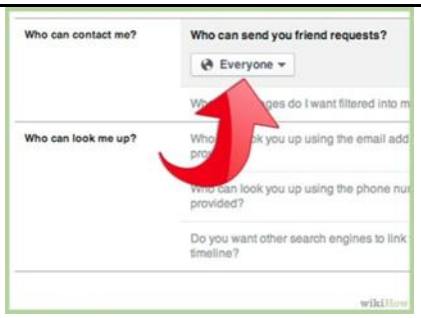
Method 3 of 4: Using the Privacy Page

Click on "Account" from the upper right hand corner and choose "Privacy Settings".

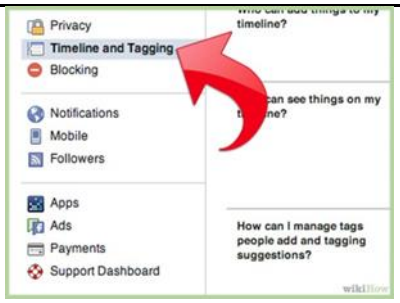
Choose a default privacy setting for your profile. This will be the setting on all your posts unless you specify otherwise.



Decide "How you Connect." Here you can make your wall and profile completely public or completely private. This offers more security than the past Facebook privacy settings allowed, as you can now further customize who can send you friend requests and messages.

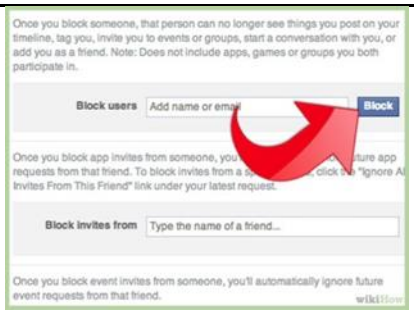


Decide "How Tags Work." Under this option, you can control who sees things that you are tagged in.



a) Turn on or turn off profile review. If profile review is on, you must approve tags before they will appear on your profile. Until you do so, the tag will appear as "pending." Remember that not approving the post doesn't mean that you're not tagged—-it simply means that the tag will not appear in your profile.

- To remove your tag from a post, simply click the "remove tag" button under the post.
- Choose who can see posts that you're tagged in. Choose from the options in the drop down menu, or create your own option by clicking "Custom."
- Decide whether or not to enable tag suggestions. When your friend uploads a photo that looks like you and this feature is enabled, Facebook will suggest that they tag you. The tag will only appear if your friend approves it.
- Enable or disable tagging from the "places" app. Leaving this option enabled will allow your friends to tag you with them when they check in to places. You will always be notified when friends check you in with them, and you have the ability to remove the check-in from your profile.
- Turn on Tag Review. Turning on tag review will allow you to review any tags your friends add to your profile before the tags appear.

Click the "Edit settings" button to the right of the "Timeline and Tagging" option. Here you can edit who can post on your timeline, who can see what others post on your timeline and who can see posts you've been tagged in. You'll also get a few options to turn on options for "Review posts friends tag you in before they appear on your timeline" and that of "Review tags friends add to your own posts on Facebook" along with "who's seeing tag suggestions when photos that look like you are uploaded" (rarely looked at).	
Use the same drop-down process to find out how much information you'd like to allow Facebook users and your friends to access.	
Limit the audience for past posts. Clicking this option will allow you to easily standardize who sees all of your past posts. By clicking "Limit Old Posts." you automatically set your past posts to your default privacy setting. • Bear in mind that if you change your mind later, you'll have to individually go back and change each post's privacy settings. If you're sure that this is what you want to do, hit "Confirm".	
Manage your blocked list settings. Here, you can block anyone from your profile (this means that it will appear to them as if you've deleted your profile). • To block someone, simply type a name or email address into the boxes provided. • To unblock someone, hit "Unblock" by their name on the list provided. • You can also block all invites to events and apps from specific friends without completely blocking the friend. To do so, type their name into the provided box.	

Policy Amendment Form

To be used by all staff across the Trust, for amendment, insertion/deletion as required.

Any amendments for submission are to be raised on this form and passed via the Principal for consideration, who will then arrange for the amendment to be presented to the Policy Board for their review, inclusion or rejection/re-submission within the Policy.

1	Copy the text for amendment into this section as per the Policy.				
2	Re-type the text as amended, for review, inclusion or rejection, for Board consideration.				
3	Reasons for amendment to be entered here in full.				
4	Seen by Academy Principal.				
	Date		Signature		
	Comments				
5	Seen by Policy Board on:				
	Date		Signature		
	Result	Reject		Include	
	Reasons				
	Remarks				
6	To be included and amended into the Policy by:				
	Date		Responsible		
	Appointment		Signature		