The GORSE Academies Trust E Safety and Online Policy

Designated Staff:	Trust Director of Digital Strategy/Partnership Director SEND/Inclusion
Reviewed by:	Governors Policy Committee
Date:	November 2023
Version:	1.4

GORSE

The GORSE Academies Trust (TGAT) E Safety and Online Policy

November 2023 updates are within the following sections:
1.6,1.7,1.8, 4.13, 4.14 and appendix 2

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; however, it is important that the use of the internet and internet-enabled devices be seen as a significant responsibility for students, staff and parents/carers that must be used appropriately. For the purpose of this policy, all staff includes supply teachers, volunteers and trainee teachers undertaking training through the Trust's school-centred initial teacher training (SCITT) programme.

1.3 It is essential that all staff, students and parents/carers from the Trust establishment are alert to e and online safety and the possible risks when using the internet and internet enabled devices. 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 is considerable and the Trust approach to online safety empowers each educational establishment to protect and educate students and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate concerns where appropriate.

1.5 E-safety covers the use of the internet as well as mobile phones, electronic communications technologies and the use of social media and social networks.

1.6 Staff members at a Trust establishment have a responsibility in accordance with the most up to date guidance: *Keeping Children Safe in Education* (KCSiE) and the *Guidance for Safer Working Practice for those working with Children and Young People in Education Settings*, to safeguard students and report abuse immediately to designated staff members, as per the Trust's Safeguarding and Child Protection Policy. All staff will attend child protection training, including e-safety training which, includes an understanding of the expectations, applicable roles and responsibilities in relation to filtering and monitoring (see appendix 2). Training requirements are outlined in the Trust's Safeguarding & Child Protection Policy.

1.7 The Designated Safeguarding Lead (DSL) will take lead responsibility for safeguarding and child protection (including online safety and understanding the filtering and monitoring systems and processes in place), and ensure that staff have the relevant skills and knowledge to safeguard children effectively.

1.8 This policy has also been informed by the LCC Guidance for Staff working in Educational Settings on the Use of Digital Technologies and Social Media (2020); CEOP (Child Exploitation and Online Protection); the Communication Act 2003, DFE guidance document: Preventing and Tackling Bullying and Cyberbullying 2017; guidance via the UK Safer Internet Centre (UKSIC), Meeting Digital and Technology Standards in Schools and Colleges, DFE 2023 and should be read in conjunction with the following Trust policies:

- Safeguarding and Child Protection
- Working from Home
- Remote Learning
- Relationships, Sex and Health Education (RSHE)
- Professional Principles
- Safer Recruitment
- Staff Disciplinary
- GDPR and Data Security
- Behaviour & Positive Discipline
- Anti-bullying and Hate Crime/Incident

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

1.10 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.

1.11 The Trust will ensure that Governors and all staff, including supply staff and volunteers will receive formal on-line safety training in order to understand their responsibilities and discharge their duties.

1.12 In order to 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, the Trust will appoint an e-safety officer.

1.13 Each Trust establishment will also 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 THE E-SAFETY POLICY

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

2.2 The policy will define the code of conduct for staff and students 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 The policy outlines the responsible approach adopted to educating students in online safety/digital literacy through a broad, relevant and progressive curriculum.

2.5 This policy is available on each Trust establishment's website for access by parents/carers, staff, students and wider stakeholders.

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

2.7 The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

- **Content:** being exposed to illegal, inappropriate or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalization and extremism
- **Contact:** being subjected to harmful online interaction with other users, for example: peer-to-peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes
- **Conduct:** personal online behaviour that increases the likelihood of, or causes harm, for example: making, sending and receiving explicit images (e.g. consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and
- **Commerce:** risks such as online gambling, inappropriate advertising, phishing and/or financial scams. Concerns can be reported to the Anti-Phishing Group https://apwg.org/

3. ROLES and RESPONSIBILITIES

3.1 Governors

Governors are responsible for the approval and adoption of the E-safety and Online Security Policy and for reviewing the effectiveness of the policy. Governors receive regular information about on-line safety incidents and receive monitoring reports. A member of the Governing Body is appointed to the role of Safeguarding Governor. The role will include, but is not limited to:

- Regular meetings with the Trust establishment's DSL, who is the delegated e-safety officer
- Regular monitoring of online safety incident logs

- Regular monitoring of filtering/change control logs
- Reporting to relevant Governors/Board/Committee meetings

3.2 **Principals and Senior Leaders**

- The Principal has a duty of care for ensuring the safety (including e-safety) of members of the school community; day-to-day responsibility for e-safety will be delegated to the DSL, who will act as the establishments e-safety officer
- The Principal and (at least) one other member of the Senior Leadership Team should be aware of the procedures to be followed in the event of a serious online allegation being made against a member of staff (refer to the flow chart: Online Safety Incidents in section 4.18.3)
- The Principal and Senior Leaders are responsible for ensuring that the e-safety officer and other relevant staff receive suitable training to enable them to carry out their e-safety role and to train other colleagues, as necessary
- The Principal and Senior Leaders will ensure that systems are in place to allow for monitoring and support for staff undertaking the internal e-safety officer role
- The Senior Leadership Team will receive regular monitoring reports from the E-Safety Officer

3.3 **E-Safety Officer**

- Takes day-to-day responsibility for online safety issues and has a leading role in establishing and reviewing the Trust establishment's online safety documents and policies
- Works closely with the Trust's Director of Safeguarding, who will be able to advise in online safety issues and provide guidance relating to child protection and safeguarding
- Ensures that all staff are aware of the procedures that need to be followed in the event of an online safety incident taking place
- Provides training and advice for staff and maintains an audit of training need and training completed
- Liaises with Network Managers/Technical staff and Trust's Director of IT
- Receives reports of online safety incidents and creates a log of incidents to inform future online safety developments
- Meets regularly with the Safeguarding Governor to discuss current issues and review incident logs and filtering/change control logs

3.4 **Teaching and Support Staff**

Are responsible for ensuring that:

- They have an up-to-date awareness of online safety matters and of the current Trust establishment online safety policy and practices
- They have read, understood and signed the staff acceptable use policy

- They report any suspected misuse or problem to the Principal/Senior Leader/e-safety officer/Designated Child Protection Lead for investigation
- All online safety issues are embedded in all aspects of the curriculum and other activities
- Students understand and follow the E-Safety and Online Security Policy and acceptable use polices
- Students have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations
- They monitor the use of digital technologies and mobile devices within lessons and implement current policies with regard to these devices
- In lessons where internet use is pre-planned, students should be guided to sites checked as suitable for their use and that processes are in place for dealing with any unsuitable material that is found on internet sites

3.5 **Students**

- Are responsible for using the Trust establishment digital technology systems in accordance with the student acceptable use agreement
- Understand the need to avoid plagiarism and uphold copyright regulations
- Understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so
- Know and understand policies on the use of mobile devices and digital cameras, which extends to taking/use of images and on-line bullying
- Should understand the importance of adopting good online safety practice when using digital technologies out of school and know that the Trust establishment's e-safety and online security policy covers their actions out of school, if related to their membership of the school

3.6 **Parents/Carers**

Parents/carers play a crucial role in ensuring that their children understand the need to use the internet/mobile devices in an appropriate way. The Trust establishment will take every opportunity to help parents/carers understand these issues through parent's evenings, newsletters, letters, information located on the Trust establishment website, communications, social media and information about local and national online safety campaigns and literature. Parents and carers will be encouraged to support the Trust establishment in promoting good online safety practice.

3.7 **Community Use**

Community Users who access Trust establishment systems or programmes as part of the wider Trust establishment provision will be expected to sign and adhere to a Community User Acceptable Use Agreement before being provided access to Trust establishment systems.

4. PROFESSIONAL EXPECTATIONS OF STAFF

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

4.2 Staff members at each Trust establishment 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.

4.3 Staff who are provided with a laptop or tablet by the Trust establishment must use this only for academic purposes. These remain the property of the Trust establishment and open to scrutiny by Senior Leaders, and all internet traffic will be monitored both on and offsite.

4.4 All staff members are responsible for their personal use of social media, networks and electronic devices 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 Trust and its establishments.

4.5 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.

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

4.7 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 Trust establishment.

4.8 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 Trust establishment 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, and ex–students in this way, without consent from the Principal, may be subject to disciplinary action.

4.9 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/carer 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.

4.10 Safe and professional behaviour of staff online will be discussed at 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 Trust establishments cannot be isolated from your working life. Comments about the Trust, Trust establishments, students, parents/carers or colleagues can bring the Trust and Trust establishments into disrepute and make both the Trust establishment and the employee liable to legal action.

4.11 **Appropriate computer usage**

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

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

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

4.11.4 Only members of IT Services 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.

4.11.5 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.

4.12 **Social media and networks**

4.12.1 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 Trust establishment.

4.12.2 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 immediately.

4.12.3 If a member of staff coincidentally 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.

4.12.4 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.

4.12.5 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.

4.12.6 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.

4.12.7 All staff 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.

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

4.12.9 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.

4.12.10 Any material which is posted on social media and networks which is considered to bring the Trust and Trust establishment 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 (if applicable).

4.12.11 Staff members should not refer 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.

4.12.12 While access to social media sites through the Trust establishment network is blocked to employees, accessing the internet through mobile phones and other mobile devices is prohibited, without prior approval from the Principal, during working hours. Staff members should never use Trust establishment networks or equipment to access or update a social media site, unless this is with prior approval, for example, to post on the establishments X (Twitter) account.

4.13 **Social Media Networks and Social Media Platform Device advice**

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 Social Media networks application 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 Trust establishment email address as your email contact
- Report any threats of violence or other inappropriate posts/images to Social Media networks or to the relevant authorities, such as the Child Exploitation and Online Protection Centre (CEOP) 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
- Don't ever announce on your wall that you are going away. Many cases of burglaries are supported through these disclosures on Social Media networks

4.14 **Internet Use**

All Trust staff must adhere to the Acceptable Use/Unacceptable Use agreement, which details the expectations placed on staff, which are outlined within this policy. As a general principle, internet access is provided to employees to support work related activities. The following list is not intended to be an exhaustive list, but sets out broad areas of use that the Trust considers to be acceptable uses of the internet.

Trust web filters are assessed annually as a minimum against the http://testfiltering.com/ website as recommended by the UK Safer Internet Centre, and filtering and monitoring standards which set out that schools and colleges should:

- Review filtering and monitoring provision at least annually

The certificates for these tests are then stored for records. The tests are also carried out again if we have a major change to web filtering or a change in KCSIE/Government guidance.

4.14.1 **Acceptable Use**

Will include but not limited to:

- To provide communication within the Trust establishment via email or the website
- To provide communication with other schools and organisations for educational purposes
- To distribute details regarding Trust establishment meetings
- To provide electronic methods of communication
- Any other use that directly supports work related functions

4.14.2 **Unacceptable Use**

The following uses will be regarded as not acceptable irrespective of the means of internet access and will include, but not limited to:

- Using the computer to perpetrate any form of fraud, or software, film or music piracy
- Use for racial, sexual, homophobic or other harassment
- To access pornographic, obscene or illegal material
- To solicit personal information with the intent of using such information to cause emotional or physical harm
- Entering into a commitment on behalf of the Trust establishment (unless you have explicit permission to do this)
- Visiting internet sites that contain obscene, hateful, pornographic or otherwise illegal material
- Downloading commercial software or any copyrighted materials belonging to third parties, unless this download is covered or permitted under a commercial agreement or other such licence

- Hacking into unauthorised areas
- Publishing defamatory and/or knowingly false material about any Trust establishment, colleagues and/or our students on social networking sites, 'blogs' (online journals), 'wikis' and any online publishing format
- Revealing confidential information in a personal online posting, upload or transmission, including financial information and information relating to our students, staff and/or internal discussions
- Use of personal email to communicate with or about any students
- Introducing any form of malicious software into the corporate network
- To disrupt the work of other users, for example, includes the propagation of computer viruses

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

4.15.1 Under no circumstances should staff use their own personal devices to contact students or parents/carers either in or out of working hours, unless with the express consent of the Principal; in these circumstances, the withheld number function must be used.

4.15.2 Staff are not permitted to take photos or videos of students on personal devices. If photos or videos are being taken as part of the Trust establishment curriculum or for a professional capacity, the Trust establishment equipment will be used. Any device which takes images, videos, moving images should not be used during working time as this unless it is specifically agreed by the Principal and the device is used for work purposes that do not involve video, images or photographs.

4.15.3 The use of personal equipment within the Trust establishment can only be authorised by the Principal or Senior Leadership Team in order to comply with Safer Working Practice guidance, General Data Protection Regulations and Trust policies related to safeguarding.

4.15.4 Any breach of the Trust E-Safety and Online Policy may result in disciplinary action against that member of staff. More information on this policy can be found in the TGAT Safeguarding and Child Protection Policy and Staff Disciplinary Policy.

4.16 **Inappropriate material**

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 and staff conduct. 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.

4.17 **Illegal material**

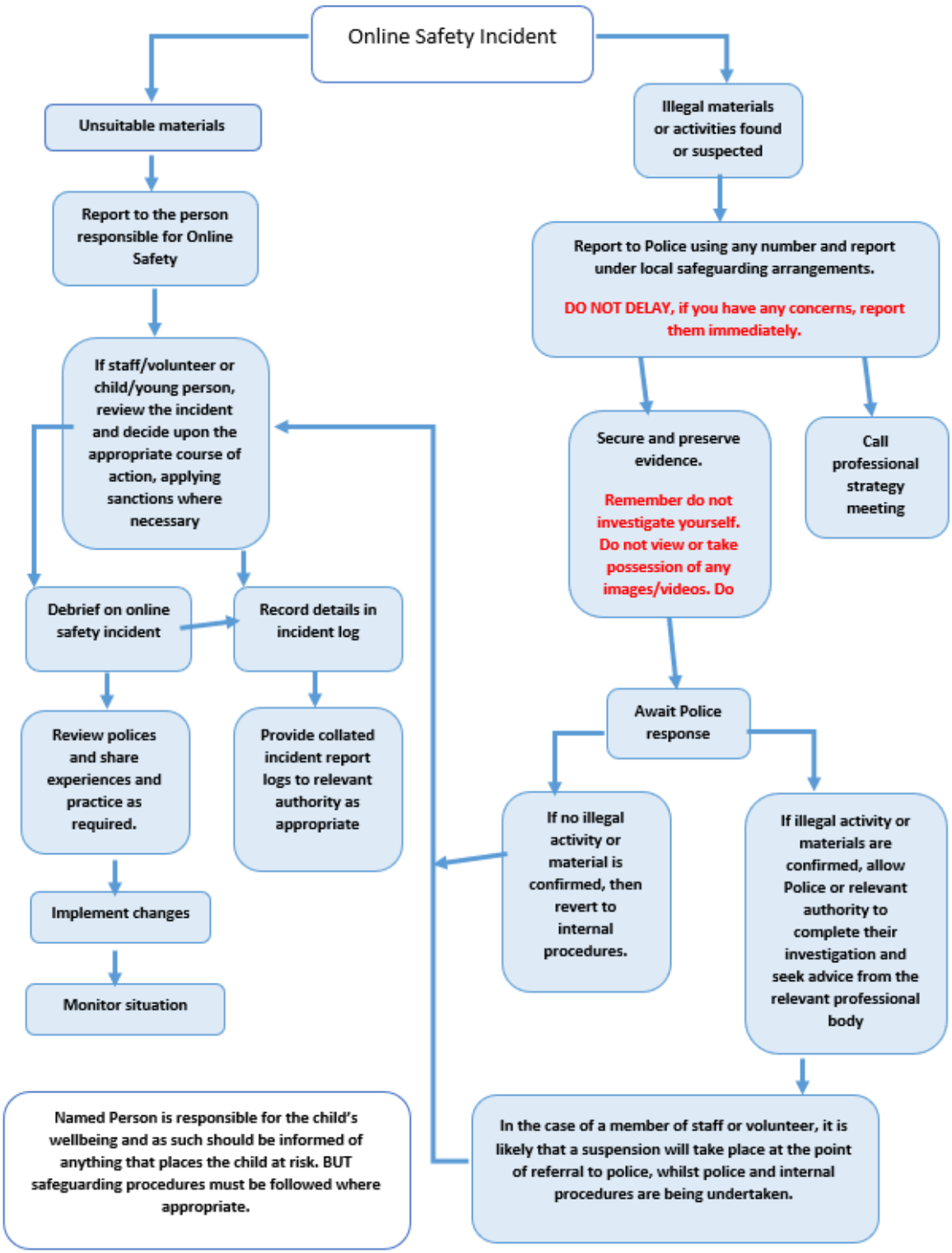
It is illegal to make, possess or distribute indecent images of a person under the age of 18 and viewing these images online may constitute possession of these images even if they are not saved. Accessing indecent images, real or doctored, of children or students on the internet or making, storing or 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 children.

4.17.1 **Illegal incidents**

If there are any suspected illegal materials or activities found or suspected, report immediately to the Police, and report under local safeguarding arrangements. Refer to the Online Safety Incident flowchart:

GORSE


Online Safety Incident
Unsuitable materials
Report to the person responsible for Online Safety
If staff/volunteer or child/young person, review the incident and decide upon the appropriate course of action, applying sanctions where necessary
Debrief on online safety incident
Record details in incident log
Review polices and share experiences and practice as required.
Provide collated incident report logs to relevant authority as appropriate
Implement changes
Monitor situation
Named Person is responsible for the child's wellbeing and as such should be informed of anything that places the child at risk. BUT safeguarding procedures must be followed where appropriate.
Illegal materials or activities found or suspected
Report to Police using any number and report under local safeguarding arrangements.
DO NOT DELAY, if you have any concerns, report them immediately.
Secure and preserve evidence.
Remember do not investigate yourself. Do not view or take possession of any images/videos. Do
Call professional strategy meeting
Await Police response
If no illegal activity or material is confirmed, then revert to internal procedures.
If illegal activity or materials are confirmed, allow Police or relevant authority to complete their investigation and seek advice from the relevant professional body
In the case of a member of staff or volunteer, it is likely that a suspension will take place at the point of referral to police, whilst police and internal procedures are being undertaken.

4.18 **Materials which incite hate, harm or harassment**

There are a range of offences in relation to incitement of hatred on the basis of ethnicity, gender, sexual orientation, sex, 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 of a hate crime. For further details, refer to the Trust Anti–Bullying and Hate Incidents Policy.

4.19 **Professionally appropriate material**

4.19.1 Trust establishment staff members should not use any equipment belonging to the Trust establishment to access adult pornography and personal equipment/devices with links and images should not be brought into the Trust establishment.

4.19.2 Trust staff should be aware that actions outside of the Trust establishment 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 Trust or Trust establishment
- Posting unprofessional comments about one's profession
- Making inappropriate statements or using offensive or hate based language.

4.20 **Confidentiality and Data**

4.20.1 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 Trust establishment 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, which means that sharing of information is in the best interests of the student.

4.20.2 Confidential information should only be stored on Trust establishment systems and devices 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.

4.20.3 Any data handled or stored by any Trust establishments is done so in accordance with the TGAT GDPR and Data Security Policy, each Trust establishment has a designated Chief Privacy Officer (CPO) that ensures the policy is upheld at their establishment.

4.20.4 **Confidentiality and Security**

4.20.5 The storing and processing of personal information is governed by the General Data Protection Regulation and Data Protection Act 2018. Employers are required to provide

clear advice to staff about their responsibilities under this legislation so that, when considering sharing confidential information, the principals set out in this legislation apply.

4.20.6 Members of staff may have access to confidential information about students and families and the organisation in order to undertake their everyday responsibilities and, in some circumstances, this may be highly sensitive or private information. Such information should only be shared when legally permissible to do so and in the interest of the student. Records should only be shared with those who have a legitimate professional need to see them.

4.20.7 Only authorised school-based devices and systems should be used to store and transfer confidential information. Developments in technology have improved the security of e-mail. This has meant that Leeds City Council have been able to follow centrally issued guidance to protect personal and special category data sent by standard e-mail. When e-mail services are configured appropriately at both ends of the route, e-mail is just as good as Mail Express or any other secure data transfer mechanism once controls are in place.

4.20.8 For further guidance in relation to sending personal information electronically, please refer to the guide for schools, Exchanging Data Electronically (December 2018). Members of staff found to be compromising confidentiality by use of unauthorised systems and devices could be subject to disciplinary action.

4.20.9 For further information in relation to confidentiality issues and safe storage of data, please refer to the Safer Working Practice Guidance for those working with Children and Young People in an Educational Setting (May 2019).

4.21 **Cyberbullying – Expectations of Colleagues**

4.21.1 Cyberbullying, bullying, harassment, defamatory comments, offensive correspondence and hate incidents within and outside the Trust establishment will not be tolerated and any member of staff found to be behaving in this manner will be dealt with in accordance with the Anti-bullying and Hate Incidents Policy, staff code of conduct and the TGAT Whistleblowing Policy (as appropriate). This may lead to disciplinary action and, in specific circumstances, will be considered a criminal offence.

4.21.2 Cyber bullying consists of threats, harassment, embarrassment, humiliation, defamation or impersonation and could take the form of general insults, prejudice-based bullying, or discrimination through a variety of media. Media could include email, Virtual Learning Environments, chart rooms, web sites, social networking sites, mobile and fixed-point phones, digital cameras, games and virtual world sites.

4.21.3 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 the Principal. The victim will be offered support and this will be fully investigated and the relevant Trust policies followed, a referral may be made to the appropriate authorities if deemed appropriate.

4.21.4 Members of staff are required to take steps to protect themselves and their personal information by:

- Keeping all passwords secret and protect access to their online accounts

- Not befriending students on social networking services and sites
- Keeping personal phone numbers private
- Not using personal phones to contact parents/carers and students
- Keeping personal phones secure, i.e. through the use of a pin code
- Not posting information about themselves that they would not want employers, colleagues, parents/cares or students to see
- Not retaliating to any incident
- Keeping any evidence of an incident
- Promptly reporting any incident using existing routes for reporting concerns

4.22 **Trust Establishment email accounts, etiquette and appropriate use**

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

4.22.2 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 through 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 it is a matter is urgent. Staff should try to respond to email requests as efficiently as possible, however, where possible staff are encouraged to have more face-to-face communication with colleagues.

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

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

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

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

5.1 Photographs, images of students' work and recorded images are part of daily school 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 collective pride 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.

5.2 Under the General Data Protection Regulations 2018 images of students and staff will not be displayed in public, either in print or online, without parent/carer permission. On admission to the Trust establishment, parents/carers will be asked to sign consent form(s) relating to the use of student photographs, images of students' work and

recorded images. The Trust establishment does this so as to prevent repeatedly asking parents/carers for permission over the academic year.

5.3 Parents/carers can withdraw their consent at any time in writing, without giving a reason. Trust establishments will comply with parent/carer wishes and will make every effort to remove existing images wherever they have been published.

5.4 The Trust processes biometric data of students and staff to provide access to specific systems (printing and cashless catering). Biometric data is only processed with prior consent from the parent/carer of the student and is stored in an anonymised fashion. This data can also be removed at any time with a request from the parent/carer.

5.5 Images of students must not be displayed or distributed, for example, in a newsletter or website, without parent/carer permission.

5.6 All images and video content including students is processed with prior consent. If consent is to be withdrawn, the Trust establishment would follow processes as set out in the TGAT GDPR and Data Security policy.

5.7 **Using photographs of students**

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

5.7.2 It is important that published images do not identify students or put them at risk of being identified. Only images created by or for the Trust establishment will be used in public and students may not be approached or photographed while in the Trust establishment or undertaking school activities without the Trust establishment's explicit permission.

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

5.7.4 All images of students are processed and stored in accordance with the General Data Protection Regulation 2018, and following the TGAT GDPR and Data Security policy.

5.7.5 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).

5.7.6 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.

5.7.7 Events recorded by family members of the students, such as Trust establishment productions or sports events, must be for personal use and only at the discretion of the Trust establishment and Principal.

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

5.7.9 Any photographers that are commissioned by the Trust establishment will be fully briefed on appropriateness in terms of content and behaviour. The photographer will

wear identification at all times, will not have unsupervised access to the students, and will be supervised by a member of staff. For more information on Trust safeguarding procedures, please refer to the TGAT Safeguarding and Child Protection Policy.

5.7.10 Child protection designated officers are aware of students who need protection and who would be put at risk if their image is used and will ensure that members of staff are made aware of students who cannot have their image published in any form.

5.8 **Complaints of misuse of photographs or video**

Parents/carers should follow the Trust Complaints Policy if they have a concern or complaint regarding the misuse of photographs. Any issues or sanctions will be dealt with in line with the relevant Trust policy.

6. CONSEQUENCES OF INAPPROPRIATE ACTION BY MEMBERS OF STAFF

6.1 The Trust may exercise the right to monitor the use of the Trust establishment computer systems, including access to websites, the interception of email and the deletion of inappropriate materials without the consent of the member of staff. This extends to the remote monitoring of Trust owned devices when outside of the Trust establishment setting.

7. TEACHING AND LEARNING THROUGH ICT

7.1 E and online safety is integrated into the curriculum in every circumstance where the internet or technology are being used, and during Personal, Social, Health and Economic Education (PSHE) lessons where modules relating to: managing risk and personal safety/social influences/media literacy and digital resilience is being taught; refer to the Trust's Relationships, Sex and Health Education Policy (RSHE) for further details with regards to the taught curriculum and specific E and online safety education.

7.2 Students will be taught 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 during PSHE/RSHE. The breadth of issues covered within the taught RSHE curriculum can be categorised into four areas of risk:

- **Content**: being exposed to illegal, inappropriate or harmful materials
- **Contact**: being subject to harmful online interaction with other users
- **Conduct**: personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce**: being at risk from online gambling, inappropriate advertising, phishing and/or financial scams

  Students will be taught (age and stage appropriately):

  - How photographs can be manipulated
  - The importance of keeping personal information private
  - About safe social networking and chat rooms

- Ownership of personal images and the risks sharing intimate nude and semi-nude images
- What constitutes a healthy relationship online
- The characteristics of abusive behaviours online
- Awareness of exploitation both sexual and criminal
- The skills to challenge or seek support for financial exploitation online
- How to develop media literacy and digital resilience
- The implications of inappropriate posts on career progression and employment

7.3 The internet is used in each Trust establishment to raise educational standards, promote student achievement, support the professional standards of the work of staff members and to enhance the Trust establishment'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.

7.4 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. This is supported by internet security, web filtering and pre-exchange checks.

7.5 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

7.6 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 and provide personalised access to learning.

7.7 For members of 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 and assessment tracking.

7.8 Engagement with parents/carers is integral to the work of members of staff and ICT gives parents/carers access to the Trust establishment website pages with a wide variety of information and resources.

7.9 **Learning to evaluate internet content**

7.9.1 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.

7.9.2 Plagiarism is dishonest/academic cheating and not consistent with our values and ethos (see also The GORSE Academies Trust Non-Examinations Assessment Policy), the Trust establishment 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 Policy. If plagiarism has occurred during an exam or a piece of coursework, the student may be prohibited from completing that exam.

7.9.3 The Trust establishment 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 Trust establishment E-safety Officer and IT Technicians. All Trust establishment's filtering is installed in accordance with the most recent version of Keeping Children Safe in Education.

7.9.4 Any material found by members of the Trust establishment 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.

8. MANAGING VIDEO CONFERENCING AND WEBCAM USE

8.1 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.

8.2 All student/teacher communication via video conferencing must be carried out over the Trust's preferred provider and in accordance with the TGAT Working from Home policy 2020.

9. EDUCATION AT HOME

9.1 Where students are expected to learn remotely at home, online teaching will follow the same principles as set out in the most up to date guidance for safer working practice for those working with children and young people in education settings (National Safer Recruitment Consortium) and DFE guidance safeguarding-and-remote-education. The use of any online learning tools and systems is in line with privacy and data

protection/GDPR requirements. The remote learning policy details expectations of staff and students.

10. SOCIAL NETWORKING, SOCIAL MEDIA AND PERSONAL PUBLISHING

10.1 Personal publishing tools include blogs, wikis, social networking sites, bulletin boards, chat rooms and instant messaging programs and (X) Twitter. These online forums are the more obvious sources of inappropriate and harmful behaviour and where students are most vulnerable to being contacted by an abusive person.

10.2 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 their Trust establishment.

10.3 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 PSHE about the risks and responsibility of uploading personal information and possible long-term implications of this information being in the public domain.

10.4 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 Positive Discipline Policy regarding the use of ICT, technology and behaviour online.

10.5 Any websites that are to be used in lessons will be risk-assessed by the teacher prior to the lesson to ensure that the website is age-appropriate and safe for use.

10.6 Official blogs created by staff or student/student groups will be password-protected and will be incorporated on the Trust establishment website with prior approval of the Principal.

10.7 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 the Trust and Trust establishment at all times and must act appropriately.

11. EQUAL OPPORTUNITIES

11.1 The Trust believes that it is essential that everyone can have access to ICT and that learning opportunities should be provided for all students, regardless of their ability, ethnicity, age, gender, sex, gender identity, beliefs, values, religion, culture and whether they have a Special Educational Need and/or Disability (SEND).

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

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

12. MONITORING

12.1 All internet traffic and use is monitored on Trust equipment both on and off site. 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.

12.2 Active Monitoring is in place on all Trust owned equipment and supported by an accredited safeguarding provider. All incidents are raised with the local safeguarding teams and a full communication protocol is in place for deployment. Appendix 2 outlines the filtering and monitoring in place across the Trust establishment devices.

13. MOBILE PHONES AND PERSONAL DEVICES - STUDENTS

13.1 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 student use of mobile phones to video and take photographs of other students and staff members for use in Cyberbullying. Devices with integrated cameras can lead to safeguarding, bullying and data protection issues. Mobile phones can also be used by students to access inappropriate internet material. If taken into the Trust establishment, they can be a distraction in the classroom and are valuable items that could be stolen, damaged, or lost.

13.2 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 face sanctions in accordance with the Trust Positive Discipline and Behaviour Policy. For more information on the Trust establishment's disciplinary sanctions, read the Trust's Positive Discipline and Behaviour Policy.

13.3 Images or files should not be sent between mobile phones in the Trust establishment 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.

13.4 The Positive Discipline and Behaviour Policy for each phase establishes the expectations with regards to student use of mobile phones and devices and can be accessed on the Trust establishment website.

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

13.6 Students who breach the Positive Discipline and Behaviour Policy relating to the use of mobile phones and personal devices will be disciplined in line with this policy.

13.7 Students are under no circumstances allowed to bring mobile phones or personal devices into examination rooms. If a student is found with a mobile phone or personal device 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.

14. MANAGING INFORMATION SYSTEMS

14.1 A designated member of staff 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 data seriously and Trust establishment networks are protected, as far as is practicably possible, against viruses, hackers and other external security threats. The security of the information systems and users will be reviewed regularly by the Network Managers, and virus protection software will be updated regularly.

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

14.3 Trust establishments undergo external penetration testing to ensure that Trust establishment networks remain secure and implement the most appropriate levels of cyber security.

15. EMAILS

15.1 Students should be aware that Trust establishment email accounts should only be used for Trust establishment-related matters. Students and parents/carers should only be contacted via an approved Trust email account. The Trust establishment has the right to monitor emails and their content, but will only do so with good reason.

16. CYBER-BULLYING

16.1 Cyber-bullying 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 abusive text messages or emails, rumours sent by email or posted on social networking sites, and distributing embarrassing pictures, videos, websites or fake profiles.

16.2 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 programs in place to prevent and tackle bullying can be found in the Trust's Positive Discipline Policy and Anti-bullying and Hate Crime and Incidents Policy. All students should be made aware of their rights and responsibilities with regards to bullying.

16.3 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. These members of staff will investigate the matter fully, provide support for the victim and alleged perpetrator (as appropriate) to act restoratively and apply sanctions when necessary.

16.4 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.

16.5 Any allegations of cyber-bullying by students will be managed in accordance with the Trust's Anti-bullying and Hate Incident Policy and Positive Discipline and Behaviour Policies.

17. PUBLISHED CONTENT AND THE TRUST ESTABLISHMENT WEBSITE

17.1 Each Trust establishment website is a tool for communicating the Trust and establishment's 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 news and events. The websites are also used to celebrate whole student body and individual student achievements and for the promotion of projects, events that encourage the development of cultural capital and extra-curricular activities.

17.2 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 students and staff, copyrights and privacy policies. No personal information about students or staff will be published.

18. MANAGING EMERGING TECHNOLOGIES

18.1 Technology is progressing rapidly and new technologies are emerging all the time. Each Trust establishment will risk-assess any new technologies before they are allowed into the establishment, and the Trust 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.

19. PROTECTING PERSONAL DATA

19.1 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.

19.2 Each Trust establishment 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.

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

19.4 National Curriculum results, attendance, assessment data, registration records, SEND data, and any relevant medical information are examples of the type of data that the Trust establishment 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 exceptional education and to respond to the changing needs of students.

19.5 In line with the General Data Protection Regulations (GDPR) 2016 and the Trust's Data Protection Policy, we will follow the principles of good practice when processing data. Each Trust establishment will ensure that data is fairly and lawfully processed and only

for limited purposes. The Trust establishment will ensure that all data processed is adequate, relevant, accurate and not excessive. Data will only be kept for the regulated period of time. 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.

19.6 There may be circumstances where the Trust establishment is required either by law or in the best interests of our students/staff to pass information onto external agencies or authorities; for example, the Local Authority, OFSTED, or Children's Social Work Services. These have their own policies relating to the protection of any data that they receive or collect.

20. USING MUSIC

All music/songs must be purchased by the Trust establishment. Fair use does not allow us to use copied material, unless you are using less than 30 seconds of the track:

- In a lesson: If the song/music being used relates specifically to a part of the curriculum (e.g. a music lesson on pop music) then a pop song could be saved to the network and used as part of fair usage. However, this song should never be made available to the general public and should always be behind a secure network
- For extracurricular activities: If you require music for an extra-curricular activity, then please contact IT and your line manager as this will need to be purchased and downloaded for you
- Use on the website: Under no circumstances is it allowed for copyrighted music to be placed on our Trust establishment websites. Please ensure that you remove any music from clips that you wish to place on the website

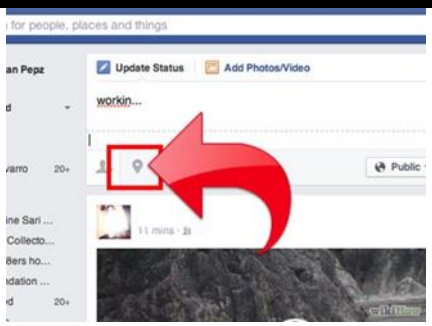
GORSE

Appendix 1 – How to Manage Facebook Privacy Options

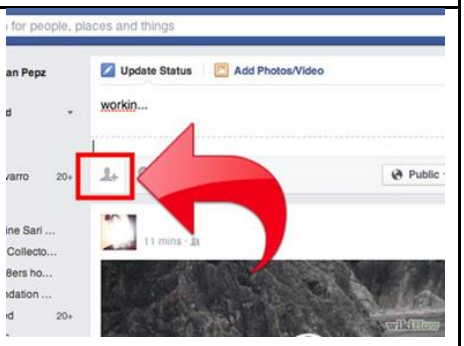
Every so often, Facebook revamps their privacy settings to make them more user-friendly. Among the most recent new features are better control of your news feed, the ability to view your profile as another user, and a simplified privacy page. Need to navigate your privacy settings? With just a few tips,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

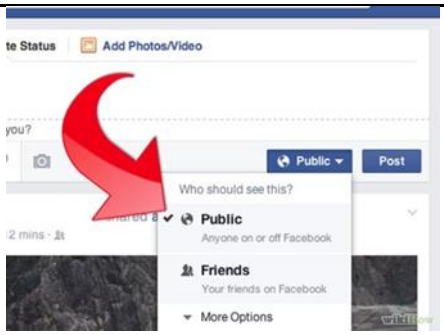
1. Type your desired status into the newsfeed bar.



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?"



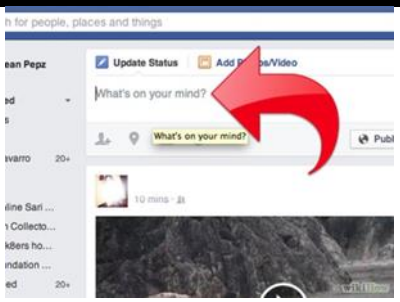
3. Decide who can see the update. Before you click Post, click the drop-down box just to the left of it. You can choose to set the status visible to the public, just your friends, or a custom set of people:
   - To make your updates available to friends of friends, click Custom, then select Friends of 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



GORSE

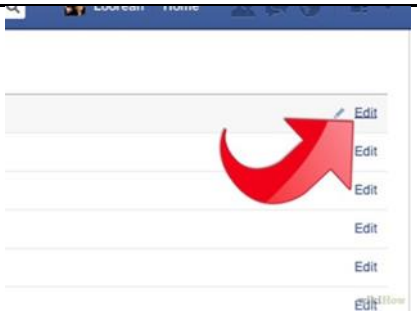
Method 2 of 4: Managing Profile Info

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 piece of 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:

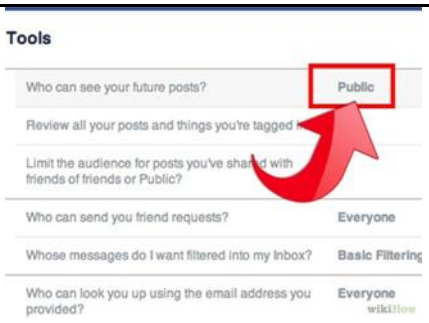
- This can differ for each post. For example, you can set your work place visible to the public, but only allow your friends to see where you went to college
- Toggle between different sections of your profile by clicking the options on the left-hand side of the page



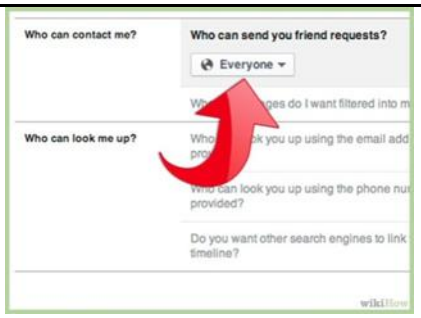
Method 3 of 4: Using the Privacy Page

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.



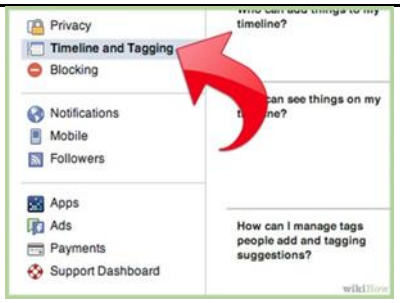
Decide "How you Connect." Here you can make your wall and profile completely public or completely private. This offers more security than the past Facebook privacy settings allowed, as you can now further customize who can send you friend requests and messages.



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

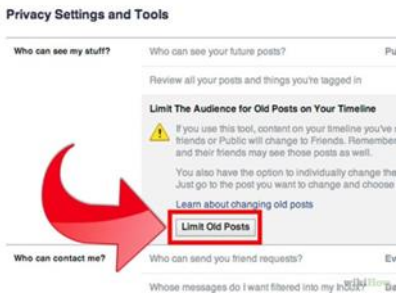


Click the "Edit settings" button to the right of the "Timeline and Tagging" option. Here you can edit who can post on your timeline, who can see what others post on your timeline and who can see posts you've been tagged in. You'll also get a few options to turn on options for "Review posts friends tag 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.

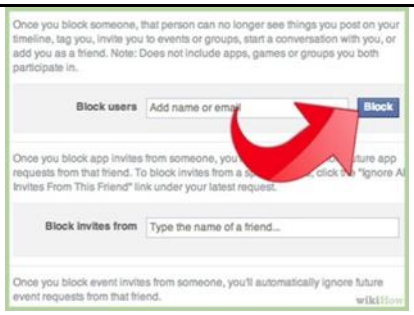
Limit the audience for past posts. Clicking this option will allow you to easily standardize who sees all of your past posts. By clicking "Limit Old Posts." you automatically set your past posts to your default privacy setting.

- 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



GORSE

Appendix 2

IT Filters and monitoring

The information below provides an assurance of our compliance with the requirements detailed in Keeping Children safe in Education relating to internet filtering and monitoring:

Extract from KCSiE 2023

141. *Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.*

142. *The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty.*

To support schools and colleges to meet this duty, the Department for Education has published filtering and monitoring standards which set out that schools and colleges should:

- *Identify and assign roles and responsibilities to manage filtering and monitoring systems*
- *Review filtering and monitoring provision at least annually*
- *Block harmful and inappropriate content without unreasonably impacting teaching and learning*
- *Have effective monitoring strategies in place that meet their safeguarding needs*

As a Trust, iBoss is used as a filtering and operating management system. This system can simultaneously manage multiple devices and different operating systems. From Google Chromebooks to Apple iOS devices, to computers running Windows, all filtering of devices must meet CIPA compliance, and iBoss has the functionality to meet this requirement. Further, to ensure students and staff have access to the information they need, the ability to provide consistent cloud access regardless of what device they are using is critical. The iBoss cloud delivers the same level of powerful filtering and user-based reporting across all users, on any device, anywhere through the cloud, eliminating the need to purchase and manage multiple solutions. What is important here is that there is **monitoring** built into this system for **all staff and students**. It is clearly specified within our E-safety and Internet Policy that staff and students are subject to the monitoring of their internet usage iBoss - Appropriate Filtering for Schools Review

To provide further safeguards for students (level 4 on the risk-assessment matrix), active monitoring is in place; Smoothwall is our current 'active monitoring provider'; Smoothwall has produced a 'Monitor Provider Checklist Response', which is published on the UK Safer Internet website, which complies with all KCSiE expectations and provides the level 4 safeguards identified in our risk assessment: Appropriate Monitoring Standards (Smoothwall)

Smoothwall provide a real-time response directly to designated safeguard trained staff to respond to and investigate.

Filtering is therefore in place on all staff and student devices, including those used remotely and all internet traffic and use is monitored in Trust equipment both on and off site (this is detailed in section 12 TGAT E-Safety and Online Policy). If required, a report can be generated detailing individual staff members' internet searches as the iBoss monitoring system can identify individual users. This is explicit in our policy e.g., if a cause for concern is raised about a staff members' internet usage, then a report could and would be generated to support any investigation.

Active monitoring by Smoothwall is in place on devices which are used by students, and can be enabled on staff devices to enable 'active monitor' staff searches. The UK Safer Internet Centre state: *Active/Pro-active technology monitoring services is deemed suitable where the risk assessment is higher* and is, therefore, wholly appropriate for students. Our risk assessments do not provide evidence that this should routinely be required for staff, and we are confident that the monitoring provided via iBoss is sufficient to comply with KCSiE guidance, especially given that it is explicit, within this guidance that the appropriateness of filtering and monitoring is a matter for individual Trust establishments.

GORSE

Appendix 3

There is a wealth of information available to support Trust establishments and parents/carers to keep children safe online. The following list is not exhaustive but should provide a useful starting point: Advice for governing bodies/proprietors and senior leaders:

- Childnet provide guidance for schools on cyberbullying
- Educateagainsthate provides practical advice and support on protecting children from extremism and radicalisation
- London Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- NSPCC provides advice on all aspects of a school or college's online safety arrangements
- Safer recruitment consortium "guidance for safe working practice", which may help ensure staff behaviour policies are robust and effective
- Searching screening and confiscation is departmental advice for schools on searching children and confiscating items such as mobile phones
- South West Grid for Learning provides advice on all aspects of a school or college's online safety arrangements
- Use of social media for online radicalisation - A briefing note for schools on how social media is used to encourage travel to Syria and Iraq
- UK Council for Internet Safety have provided advice on, and an Online Safety Audit Tool to help mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring
- Department for Digital, Culture, Media & Sport (DCMS) Online safety guidance if you own or manage an online platform provides practical steps on how companies can embed safety into the design of their online platforms. It offers information on common platform features and functions (such as private messaging) and their risks, as well as steps that can be taken to manage that risk
- Department for Digital, Culture, Media & Sport (DCMS) A business guide for protecting children on your online platform provides guidance to businesses on how to protect children on their online platform. It outlines existing regulatory requirements and provides best practice advice on how to protect children's personal data, ensure content is appropriate for the age of users, ensure positive user-to-user interactions and address child sexual exploitation and abuse

Remote education, virtual lessons and live streaming

- Case studies on remote education practice are available for schools to learn from each other

- Departmental guidance on safeguarding and remote education including planning remote education strategies and teaching remotely
- London Grid for Learning guidance, including platform specific advice
- National cyber security centre guidance on choosing, configuring and deploying video conferencing
- National cyber security centre guidance on how to set up and use video conferencing
- UK Safer Internet Centre guidance on safe remote learning

Support for children

- Childline for free and confidential advice
- UK Safer Internet Centre to report and remove harmful online content
- CEOP for advice on making a report about online abuse

Parental support

- Childnet offers a toolkit to support parents and carers of children of any age to start discussions about their online life, to set boundaries around online behaviour and technology use, and to find out where to get more help and support
- Commonsensemedia provide independent reviews, age ratings, & other information about all types of media for children and their parents
- Government advice about protecting children from specific online harms such as child sexual abuse, sexting, and cyberbullying
- Government advice about security and privacy settings, blocking unsuitable content, and parental controls
- Internet Matters provide age-specific online safety checklists, guides on how to set parental controls on a range of devices, and a host of practical tips to help children get the most out of their digital world
- Let's Talk About It provides advice for parents and carers to keep children safe from online radicalisation
- London Grid for Learning provides support for parents and carers to keep their children safe online, including tips to keep primary aged children safe online
- Stopitnow resource from The Lucy Faithfull Foundation can be used by parents and carers who are concerned about someone's behaviour, including children who may be displaying concerning sexual behaviour (not just about online)
- National Crime Agency/CEOP Thinkuknow provides support for parents and carers to keep their children safe online

- Net-aware provides support for parents and carers from the NSPCC and O2, including a guide to social networks, apps and games
- Parentzone provides help for parents and carers on how to keep their children safe online
- Parent info from Parentzone and the National Crime Agency provides support and guidance for parents from leading experts and organisations
- UK Safer Internet Centre provide tips, advice, guides and other resources to help keep children safe online

GORSE

Document control:

Reason for version change:	Policy cycle review	Version number:	1.4
Date of Approval:	November 2023	Approved by:	Policy Committee
Target Audience:	All Staff All websites	Date issued:	November 2023