The Tiffin Girls' School

ONLINE SAFETY POLICY

REVISED June 2026

Approved by: Governing Board

TABLE OF CONTENTS

Aims of the policy

1. This policy takes into account the current Department for Education's statutory guidance 'Keeping Children Safe in Education', and 'Working Together to Safeguard Children'.

2. The purpose of the Online Safety policy is to:

- Safeguard and protect all members of The Tiffin Girls' School (the School) Community online

- Identify approaches to educate and raise awareness of online safety throughout the School Community
- Enable all staff to work safely and responsibly, to model positive behaviour online and to manage professional standards and practice when using technology
- Enable all students to work safely and responsibly when using technology
- Identify clear procedures to use when responding to online safety concerns

3. In school policy, "online" refers to any activity, communication, or interaction that takes place on the internet, with AI, via digital networks, or through connected devices. It applies to both school-issued equipment and personal devices used on or off the school site

4. The School identifies that the issues classified within online safety are considerable, but can be broadly categorised into four areas of risk:
- **Content:** being exposed to illegal, inappropriate or harmful material
- **Contact:** being subjected to harmful online interaction with other users
- **Conduct:** personal online behaviour that increases the likelihood of, or causes, harm
- **Commerce**: risks such as online gambling, inappropriate advertising, phishing and / or financial scams

Scope of the policy

5. The Governing Board (GB) and the Senior Leadership Team (SLT) believe that online safety is an essential part of safeguarding and acknowledges their duty to ensure that all students and staff are protected from potential harm online.

6. The School identifies that the internet and associated devices, such as computers, Chromebooks, tablets are an important part of our teaching tools, and of everyday life. The GB and SLT believe that students should be empowered to build resilience and to develop strategies to manage and respond to risk online.

7. This policy applies to the "School Community". This means all staff and relevant volunteers including the Members of the Academy Trust, GB, SLT, teachers (including any supply or Agency staff), support staff, external contractors, visitors, volunteers and other individuals who work for, or provide services on behalf of the School (collectively referred to as "staff" in this policy) as well as students and parents/carers.

8. This policy applies to all access to the internet, use of technology and IT systems, including personal devices, or where students, staff or other individuals have been provided with School issued devices for use off-site, such as work laptops, Chromebooks, tablets or mobile phones.

9. This policy is applicable to remote learning situations as they occur.

10. The School ensure that the network and infrastructure is secure, we implement effective monitoring & filtering, and this meets the DfE's Digital Standards for 2030

Links with other policies:

11. External Policies including:
- Keeping children safe in education 2025
- Working together to safeguard children 2026
- Online Safety Act 2023
- Relationships Education, Relationships and Sex Education (RSHE) and Health Education 2025

More legislation is covered throughout this policy in their relevant sections. Some government

guidance is not statutory - instead it supports practitioners, like school staff, in the decisions we make
to keep children safe.

12. This policy links with several other policies and areas of practice including, but not limited to:

- Anti-bullying
- Artificial Intelligence Policy
- Behaviour for Learning
- Discrimination Incident Policy
- Allegations of Abuse
- Safeguarding
- Data Protection
- Relationships and Sex Education (RSHE)
- SEND
- Staff Code of Conduct
- Staff Disciplinary Policy
- Digital and AI strategy
- Photographs and Images Policy

Monitoring and review

13. Technology in this area evolves and changes rapidly. The GB will review this policy at least every year.

14. The policy will also be revised following any national or local requirements, safeguarding concerns or any changes to the technical infrastructure.

15. The School will regularly monitor internet use and evaluate online safety mechanisms to ensure that this policy is consistently applied.

16. To ensure they have oversight of online safety, the Designated Safeguarding Lead (DSL) will be informed of online safety concerns including regarding potential radicalisation.

17. The named governors for safeguarding will report on a regular basis to the GB on online safety practice and incidents, including outcomes.

18. Any issues identified via monitoring or filtering will be incorporated into any action planning.

ROLES AND RESPONSIBILITIES

19. The School recognises that all members of the School Community have important roles and responsibilities with regards to online safety.

Headteacher and Governing Board

20. The Headteacher and Governing Board will ensure that:

- online safety is viewed as a safeguarding issue and that practice is in line with national and local recommendations and requirements
- there are appropriate and up-to-date policies regarding online safety, including a Behaviour for Learning policy, which covers acceptable use of technology
- The school has appropriate filtering and monitoring systems in place on school devices and school networks, and will regularly review their effectiveness. The board will review the DfE filtering and monitoring standards, and discuss with IT staff and the safeguarding team what needs to be done to support the school in meeting the standards, which include:

- roles and responsibilities to manage filtering and monitoring systems are identified and assigned
- filtering and monitoring provisions are reviewed at least annually
- harmful and inappropriate content is blocked without unreasonably impacting teaching and learning
- effective monitoring strategies in place that meet their safeguarding needs
- a governor is appointed who will oversee online safety
- ensure that online safety is embedded within the curriculum, enabling all students to develop an age-appropriate understanding of online safety
- support the DSL and deputy DSLs by ensuring they have sufficient time and resources to fulfil their online safety responsibilities
- ensure there are robust reporting channels for the school community to access regarding online safety concerns including potential radicalisation, and including internal, local and national support
- ensure that appropriate risk assessments are undertaken regarding the safe use of technology
- audit and evaluate online safety practice to identify strengths and areas for improvement

Designated Safeguarding Leads (DSL)

21. The DSL has lead responsibility for whole school online safety with input and guidance from the DSL Years 12-13 (with specific reference to the School's Prevent duty) and the wider DSL team.

22. The DSL will:

- act as a named point of contact on all online safeguarding issues and liaise with other members of staff or other agencies, as appropriate
- ensure that online safety is recognised as part of the School's safeguarding responsibilities and that a coordinated approach is implemented
- ensure all members of staff receive regular, up-to-date and appropriate online safety training
- access regular and appropriate training and support to ensure they understand the unique risks associated with online safety (including sharing of personal data, access to illegal/inappropriate materials, inappropriate online contact with adults/strangers, potential or actual incidents of grooming, online bullying, sexting and suspicions of radicalisation) and have the relevant knowledge and up to date information required to keep students safe online
- access regular and appropriate training and support to ensure they recognise the additional risks that students with SEN and disabilities (SEND) face online
- embed online safety in the pastoral curriculum
- keep up-to-date with current research, legislation and trends regarding online safety and communicate this to the School Community, as appropriate
- ensure that online safety is promoted to parents, carers and the wider Community, through a variety of channels and approaches
- take the lead on understanding the filtering and monitoring systems providing regular assurance to governors that these systems are effective
- alongside the IT Provider the DSL will understand the technical processes to respond to safeguarding concerns
- maintain records of online safety concerns, as well as actions taken, as part of the School's safeguarding recording mechanisms
- monitor online safety incidents to identify gaps and trends, and use this data to update the education response, policies and procedures
- report online safety concerns, as appropriate, to the SLT and GB
- Oversee the process where requests are made to bypass filtering and monitoring systems for educational or school management purposes. This will be done in coordination with the AHT for Digital Strategy and the AHT DPO
- work with the SLT to review and update online safety policies on a regular basis with stakeholder input
- meet termly with the governors with lead responsibility for safeguarding and online safety

- ensure that all students have signed the Acceptable Usage agreement, including students who join after the start of Year 7

23. The DSL Years 12-13 will provide input, advice and guidance as regards online safety and the School's Prevent duty.

Staff Members

24. It is the responsibility of all members of staff to:

- read, understand, sign and adhere to the online safety and acceptable use policies, and to the Staff Code of Conduct
- read and understand the relevant sections of Keeping Children Safe in Education, as directed by the DSL
- take responsibility for the security of School systems and the data they use or have access to
- model good practice when using technology and maintain a professional level of conduct in their personal use of technology, both on and off site
- embed online safety education in curriculum delivery, wherever possible
- have an awareness of a range of online safety issues and how they may be experienced by the students in their care
- identify online safety concerns and take appropriate action by reporting these to the DSL and by following the School's safeguarding policies and procedures
- know when and how to escalate online safety issues including potential radicalisation - signposting to appropriate support, internally and externally
- follow School instructions regarding use of devices, including updating of School passwords as and when required
- Adhere to the school's AI policy and guidelines (see AI Policy) for the responsible and ethical use of AI technologies.
- monitor IT activity in lessons and in extracurricular and extended School activities
- be aware of online safety issues related to the use of mobile phones, cameras and hand-held devices and to monitor their use and implement current School policies with regard to these devices
- take personal responsibility for professional development in this area

IT provider

25. It is the responsibility of staff managing the technical environment to:

- provide technical support and perspective to the DSL and SLT, especially in the development and implementation of appropriate online safety policies and procedures
- supporting the AHT Digital Strategy Lead and AHT DPO in the reviewing of Apps and platforms from a safeguarding and data protection perspective
- implement appropriate security measures as directed by the DSL and SLT, such as password policies and encryption and up to date antivirus software to ensure that the School's IT infrastructure/system is secure and not open to misuse or malicious attack, whilst allowing learning opportunities to be maximised
- ensure that the filtering policy is applied and updated on a regular basis; responsibility for its implementation is shared with the SLT
- ensure that the monitoring systems are applied and updated on a regular basis; responsibility for their implementation is shared with the SLT
- ensure appropriate access and technical support is given to the DSL for the filtering and monitoring systems, to enable them to take appropriate safeguarding action if/when required. Monitoring systems for staff usage is completed by the DSL with reference to the HR Director when required
- Conducting a full security check and monitoring the school's IT systems on a daily basis. This includes proactive filtering and regular review of system logs to include unauthorised use of

social media networks, instant messaging applications, digital gaming environments, and restricted/illegal content platforms.

Students

26. It is the responsibility of students (at a level appropriate to their age and ability) to:

- engage in age appropriate online safety education opportunities
- read, understand, sign and adhere to the acceptable use policies
- respect the feelings and rights of others both on and offline
- take responsibility for keeping themselves and others safe online including knowing and understanding the dangers of social networking sites as well as their benefits
- understand the importance of adopting good online safety practice when using digital technologies out of School and know that the School's online safety policy covers their actions out of School
- understand the importance of reporting abuse, misuse or access to inappropriate materials, including concerns about students who may be becoming radicalised, and know how to report such abuse
- know, understand and adhere to the School's policies on use of mobile phones, use of AI, Chromebooks, digital cameras and hand-held devices, including the sanctions set out in the Behaviour for Learning policy and as notified by the School from time to time

Parents/Carers

27. It is the responsibility of parents/carers to:

- read and endorse the student acceptable computer use policy
- support the School's online safety approaches by discussing online safety issues with their children and reinforcing appropriate and safe online behaviours at home
- model safe and appropriate use of technology and social media
- identify changes in behaviour that could indicate that their child is at risk of harm online
- seek help and support from the School, or other appropriate agencies, if they or their child encounter risk or concerns online
- use School systems, such as learning platforms, and other network resources, safely and appropriately
- take responsibility for their own awareness in relation to the risks and opportunities posed by new and emerging technologies

Visitors

28. Visitors to the school site will be asked to sign a Visitor Acceptable Use Agreement which will require them to agree to the following:

- to connect to systems at The Tiffin Girls' School (the school) only using the Wi-Fi details supplied
- that websites they visit while connected to the school network will be logged automatically by the school's IT systems
- that they confirm that their device has software installed to prevent malicious software running and spreading across the school's network
- that they will not disclose the Wi-Fi password they are given to others
- that their use of IT on the school's network will be of a professional nature, and they will not use school systems for recreational use
- that they will immediately report any illegal, inappropriate or harmful material or incident they become aware of online to a member of school staff
- that they will not download personal data relating to staff or students onto any device that is not owned or managed by the school

- that if their device is able to take photographs or video, they will not take images of anyone at the school, nor will they publish such images online without permission from a senior member of staff
- that if they connect their device to a display, they will ensure that anything on screen is of a professional nature and suitable for those viewing the display in the room, or who may see it as they pass by
- that they acknowledge that the school reserves the right to remove network access for devices where they may pose a security or safeguarding risk to staff or students, or where use does not follow this policy

ENGAGEMENT

Education and engagement with students

29. The School will establish and embed a progressive online safety curriculum to raise awareness and promote safe and responsible internet use amongst students by:

- ensuring education regarding safe and responsible use precedes internet access
- ensuring staff always consider age-appropriateness when speaking of online safety and will be aware of those students who may be particularly vulnerable
-
- reinforcing online safety messages whenever technology or the internet is in use
- educating students in the effective use of the internet to research; including the skills of knowledge location, retrieval and evaluation
- Permitting students (not including Year 7) to use defined AI tools for classwork, projects, and research, provided it aligns with the educational objectives set by teachers and conforms to the guidelines outlined in the AI policy.
- making students aware that IT systems and encrypted traffic are 'inspected' for security purposes (i.e. to identify malicious activity) and this potentially exposes information such as passwords and bank details to technical staff
- teaching students:
    - to be critically aware of the materials they read and shown how to validate information before accepting its accuracy
    - the need to acknowledge the source of any information used and to respect copyright when using material accessed on the internet
    - how to recognise persuasion techniques
    - how to recognise acceptable and unacceptable online behaviour
    - how to identify online risks
    - about positive, healthy and respectful relationships online
    - about the effects of their online actions
    - how and when to seek support and
    - where to obtain help and support if they are concerned about any online content or contact including online safety in Personal, Social, Health and Economic (PSHE), Relationships and Sex Education (RSHE) and computing programmes of study
    - Specifically ensuring that our curriculum meets the requirements of the RSHE DfE Guidance (2025). Including:
        - Rights, responsibilities and opportunities online, including that the same expectations of behaviour apply in all contexts, including online.
        - Online risks, including the importance of being cautious about sharing personal information online and of using privacy and location settings appropriately to protect information online. Students should also understand the difference between public and private online spaces and related safety issues.
        - The characteristics of social media, including that some social media accounts are fake, and / or may post things which aren't real / have been created with AI. That social media users may say things in more extreme ways than they might in face-to-

face situations, and that some users present highly exaggerated or idealised profiles of themselves online.

- Not to provide material to others that they would not want to be distributed further and not to pass on personal material which is sent to them. Students should understand that any material provided online might be circulated, and that once this has happened there is no way of controlling where it ends up. Students should understand the serious risks of sending material to others, including the law concerning the sharing of images.
- That keeping or forwarding indecent or sexual images of someone under 18 is a crime,even if the photo is of themselves or of someone who has consented, and even if the image was created by the child and/or using AI generated imagery. Students should understand the potentially serious consequences of acquiring or generating indecent or sexual images of someone under 18, including the potential for criminal charges and severe penalties including imprisonment. Students should know how to seek support and should understand that they will not be in trouble for asking for help, either at school or with the police, if an image of themselves has been shared. Students should also understand that sharing indecent images of people over 18 without consent is a crime.
- What to do and how to report when they are concerned about material that has been circulated, including personal information, images or videos, and how to manage issues online.
- About the prevalence of deepfakes including videos and photos, how deepfakes can be used maliciously as well as for entertainment, the harms that can be caused by deepfakes and how to identify them.
- That the internet contains inappropriate and upsetting content, some of which is illegal, including unacceptable content that encourages misogyny, violence or use of weapons.
- Students should be taught where to go for advice and support about something they have seen online. Students should understand that online content can present a distorted picture of the world and normalise or glamorise behaviours which are unhealthy and wrong.
- That social media can lead to escalations in conflicts, how to avoid these escalations and where to go for help and advice.
- How to identify when technology and social media is used as part of bullying, harassment, stalking, coercive and controlling behaviour, and other forms of abusive and/or illegal behaviour and how to seek support about concerns. For example, see Report Remove
- That pornography, and other online content, often presents a distorted picture of people and their sexual behaviours and can negatively affect how people behave towards sexual partners. This can affect students who see pornographic content accidentally as well as those who see it deliberately. Pornography can also portray misogynistic behaviours and attitudes which can negatively influence those who see it.
- How information and data is generated, collected, shared and used online.
- That websites may share personal data about their users, and information collected on their internet use, for commercial purposes (e.g. to enable targeted advertising).
- That criminals can operate online scams, for example using fake websites or emails to extort money or valuable personal information. This information can be used to the detriment of the person or wider society. About risks of sextortion, how to identify online scams relating to sex, and how to seek support if they have been scammed or involved in sextortion.
- That AI chatbots are an example of how AI is rapidly developing, and that these can pose risks by creating fake intimacy or offering harmful advice. It is important to be able to critically think about new types of technology as they appear online and how they might pose a risk.

30. The School will enable students to read and understand the acceptable use policies in a way which suits their age and ability by:

- informing students that network and internet use will be monitored for safety and security purposes and in accordance with legislation
- rewarding positive use of technology
- providing online safety education and training as part of the transition programme across the key stages

- using support, such as external visitors where appropriate, to complement and support our internal online safety education approaches

Vulnerable Students

31. The School recognises that some students are more vulnerable online due to a range of factors. This may include, but is not limited to children in care, children who are classified as 'Children in Need' (CIN) for whom there is external services involvement, children with Special Educational Needs and Disabilities (SEND) or mental health needs, children with English as an additional language (EAL) and children experiencing trauma or loss.

32. The School will ensure that differentiated and ability appropriate online safety education, access and support is provided to vulnerable students.

33. When implementing an appropriate online safety policy and curriculum, the School will seek input from specialist staff as appropriate, including the SENCO.

Training and Engagement with Staff

34. The School will:

- provide and discuss the online safety policy and procedures with all members of staff as part of induction
- provide up-to-date and appropriate online safety training for all staff on a regular basis, with at least annual updates - this will cover the potential risks posed to students (Content, Contact, Conduct and Commerce) as well as the School's professional practice expectations
- recognise the expertise staff build by undertaking safeguarding training and managing safeguarding concerns and provide opportunities for staff to contribute to and shape online safety policies and procedures
- make staff aware that our IT systems are monitored, and that activity can be traced to individual users; staff will be reminded to behave professionally and in accordance with our policies when accessing our systems and devices
- make staff aware that IT systems and encrypted traffic are 'inspected' for security purposes (i.e. to identify malicious activity) and this potentially exposes information such as passwords and bank details to technical staff
- make staff aware that their online conduct outside of the setting, including personal use of social media, could have an impact on their professional role and reputation
- highlight useful educational resources and tools which staff should use, according to the age and ability of the students, and follow the approval process for introduction as defined in the Artificial Intelligence Policy
- ensure all members of staff are aware of the procedures to follow regarding online safety concerns affecting students, colleagues or other members of the School Community
- Ensure that staff are aware of the need to separate their personal use of platforms from their professional use
- Ensure that staff are aware of which platforms they may use for teaching and learning purposes.
- Ensure that staff are aware of the safeguarding and GDPR considerations relating to the use of AI apps and platforms, particularly in relation to the anonymisation of personal data.

Awareness and Engagement with Parents/Carers

35. The School recognises that parents/carers have an essential role to play in enabling children and young people to become safe and responsible users of the internet and associated technologies.

36. The School will build a partnership approach to online safety with parents/carers by:

- providing information and guidance on online safety in a variety of formats
- drawing their attention to the Online Safety Policy and expectations e.g. in newsletters, joining information, letters and on the School's website

- requesting that they read online safety information as part of joining our Community, for example, within our home School agreement
- educating parents re. how their children will be using AI and how they should not be using it.
- requiring them to read our acceptable use policies and discuss the implications with their children

REDUCING ONLINE RISKS

37. The School recognises that the internet is a constantly changing environment with new applications, devices, websites and material emerging at a rapid pace.

38. The School will:
- regularly review the methods used to identify, assess and minimise online risks
- examine emerging technologies for educational benefit and undertake appropriate risk assessments before use in the School is permitted
- ensure that appropriate filtering and monitoring is in place and take all reasonable precautions to ensure that users can only access appropriate material
- ensure that users are reminded to change passwords as and when required
- ensure that personal data is held and processed in compliance with the UK General Data Protection Regulation and the Data Protection Act 2018 (Data Protection Legislation) and in accordance with the School policies for data protection
- ensure that users are aware that breaches of the Data Protection Legislation and/or School policy must be reported to the School's Data Protection Officer

39. Due to the global and connected nature of the internet, it is not possible to guarantee that unsuitable material cannot be accessed via the School's computers or devices. All members of the School Community are made aware of the School's expectations regarding safe and appropriate behaviour online and the importance of not posting any content, comments, images or videos which could cause harm, distress or offence to members of the School Community. This is clearly outlined in the acceptable use policies and highlighted through a variety of education and training approaches.

40. The school manages the apps and extensions to which students have access on their Chromebooks. The school manages the websites to which students have access during school and outside of school hours. Outside of school we expect parents to help manage access to Chromebooks and how they are used in line with our acceptable use policies, including appropriate filtering via their broadband access.

SAFER USE OF TECHNOLOGY

Classroom Use

41. The School uses a wide range of technology. This includes access to:
- Computers, Chromebooks, laptops and other digital devices
- Internet, which may include search engines, educational websites and access to AI via Google Gemini (this is restricted to certain year groups only)
- Learning platform/intranet (Google Classroom)
- Email
- Digital cameras, webcams and video cameras
- Interactive screens

42. All School-owned devices will be used in accordance with the acceptable use policies and with appropriate safety and security measures in place.

43. All student-owned devices for use in the classroom will be used in accordance with the acceptable use and safeguarding policies.

44. Members of staff will always evaluate websites, tools and applications fully before use in the classroom or recommending for use at home, ensuring they follow the procedure for approval as outlined in the school's Artificial Intelligence Policy

45. The School will use age appropriate search tools following an informed risk assessment, to identify which tool best suits the needs of our School Community.

46. The School will ensure that the use of internet-derived materials by staff and students complies with copyright law and acknowledges the source of information.

47. Students will be appropriately supervised when using technology, according to their age, ability and understanding.

Managing Access

48. The IT contractor will maintain a record of users who are granted access to our devices and systems.

49. All users will have clearly defined access rights to School IT systems. Details of the access rights will be recorded by the IT department and will be shared with the Data Protection Officer (DPO) for review on an annual basis. The IT Contractor will always check with the DPO if they receive a request for access.

50. All staff and students will read and sign an acceptable use policy before being given access to the School's computer system, IT resources or internet.

Decision Making

51. The IT Contractor ensures that the School has age and ability appropriate filtering and monitoring in place, to limit student exposure to online risks.

52. The IT Contractor is aware of the need to prevent "over blocking", as that may unreasonably restrict what can be taught, with regards to online activities and safeguarding, and motivate some students to seek ways of bypassing what they see as unreasonable over-blocking.

53. The School's decision regarding filtering and monitoring has been informed by a risk assessment, considering our specific needs and circumstances.

54. Changes to the filtering and monitoring approach will be risk assessed by staff with educational and technical experience and, where appropriate, with consent from SLT; all changes to the filtering policy are logged and recorded. If the IT Contractor receives a request, they will check this with SLT (Headteacher/DSL/ AHT Digital/ AHT DPO) before making a change.

55. The DSL will ensure that regular checks are made to ensure that the filtering and monitoring methods are effective and appropriate.

56. All members of staff are aware that they cannot rely on filtering and monitoring alone to safeguard students; effective classroom management and regular education about safe and responsible use is essential.

57. Executable files can only be run with system Administrative rights.

Filtering

58. Levels of Internet access and supervision will vary according to the students' age and experience. Older students, as part of a supervised project, might need to access specific adult materials - for instance a course text or set novel might include references to sexuality - while teachers may need to research areas including drugs, medical conditions, bullying, racism or harassment. In such

cases, the restrictions imposed by the School's filtering system may be removed temporarily while the user accesses the material under close supervision.

59. The School will apply Webscreen filtering and a monitoring system.

60. Staff and students who discover that an unsuitable site is accessible must report this to the School's DSL and to the IT Contractor.

61. The IT Contractor will manage the configuration of the filtering system to ensure that it is appropriate, effective and reasonable.

62. The School will report any online material it believes to be illegal to the appropriate agencies.

63. The filtering system blocks all sites on the Internet Watch Foundation (IWF) list.

64. If students discover unsuitable sites, they will be required to report their concern to a member of staff. The member of staff will report the concern (including the URL of the site if possible) to the DSL and /or the IT Contractor and the breach will be recorded and escalated as appropriate.

65. Parents/carers will be informed of filtering breaches involving their child.

66. Any material believed to be illegal will be reported immediately to the appropriate agencies, such as the IWF, Police or Child Exploitation and Online Protection Centre (CEOP).

Monitoring

67. Acceptable use policies are underpinned by a principle of trust and this extends to the notion of individual privacy in regards to the school's network and the School's email system. Whilst we seek to maintain this trust and notion of individual privacy, there are, however, situations whereby the school is authorised to monitor or access digital content of a member of staff.

68. All members of the School Community are made aware that the School's email and internet facilities are business systems, owned by the School. The School therefore reserves the right to monitor all use of the internet and of the School's IT systems. Usage by staff and students will be monitored to ensure that the systems and all school owned or provided internet enabled devices are being employed primarily for business and educational reasons.

69. The School has proxy access to all the School's communication systems for monitoring and interception of communications in order to deal with matters in a member of staff's absence for holiday, illness or other reasons.

70. If a concern is identified via monitoring the DSL will be informed as appropriate.

71. All users will be informed that use of the systems can be monitored and that all monitoring will be in line with data protection, human rights and privacy legislation.

Managing Personal Data Online

72. Staff should not use personal emails, WhatsApp, text messages, or other forms of personal mobile platforms to communicate on School matters. This applies regardless of whether personal data might be included.

73. Personal data will be recorded, processed, transferred and/or made available online in accordance with General Data Protection Regulations and Data Protection legislation.

74. Full information on secure handling of personal data can be found in our Data Protection and Secure Data Handling policies.

75. Personal data breaches must be reported to the Data Protection Officer immediately.

Protocols on using digital and video images

76. When using digital images, staff inform and educate students about the risks associated with taking, using, sharing, publishing and distributing images. In particular, they recognise the risks attached to publishing their own images on the internet e.g. on social networking sites.

77. If any incidents come to light about youth produced sexual imagery i.e. the sharing of sexual images of students under 18, the DSL will be advised in the first instance.

78. Staff are allowed to take digital image/video/voice recordings to support educational aims, but must follow School policies concerning obtaining consent, and the sharing, distribution and publication of those images. This includes checking the list on the Google drive of staff and students where consent has not been provided. Any images should only be taken on School equipment. Personal equipment of staff should NOT be used for such purposes except for authorised use of the School's online accounts. Images for use on school social media can be taken on personal mobile phones, but taken and used only in accordance with the School's guidance on social media usage. Any images taken must be deleted immediately from any personal equipment and linked cloud storage.

79. The school may use photographs or images of students on the school website and social media but all photographs used will comply with the requirements of our Photographs and Images policy. If images are used of students these will be selected carefully and will comply with the School's protocol for gaining consent. Images of staff/students who have not given consent will not be used.

Staff will be expected to use school guidance on taking photographs in order to limit any risk of harm from their use.

Security and Management of Information Systems

80. The School takes appropriate steps to ensure the security of our information systems, including:

- Virus protection being updated regularly
- Encryption for personal data sent over the Internet or taken off site (such as via portable media storage) or access via appropriate secure remote access systems
- Not using portable media without specific permission; portable media will be checked by an anti-virus/malware scan before use
- Not downloading unapproved software to work devices or opening unfamiliar email attachments
- Regularly checking files held on our network
- The appropriate use of user logins and passwords to access the School network including regular changing of passwords where appropriate
- Specific user logins and passwords will be enforced for all
- All users are expected to log off or lock their screens/devices if systems are unattended
- Servers, wireless systems and cabling is securely located and physical access restricted

Password Policy

81. All members of staff will have their own unique username and private passwords to access our systems; members of staff are responsible for keeping their password private.

82. From Year 7, all students are provided with their own unique username and private passwords to access our systems; students are responsible for keeping their password private.

83. We require all users to:

- Use strong passwords for access into our system as per the minimum password requirements
- Change their passwords regularly
- Always keep their password private; users must not share it with others or leave it where others can find it
- Not login as another user at any time

Managing the Safety of Our Network

84. We will ensure that information posted on our website meets the requirements as identified by the Department for Education (DfE).

85. We will ensure that our website complies with guidelines for publications including: accessibility; data protection; respect for intellectual property rights; privacy policies and copyright.

86. Staff or student personal information will not be published on our website; the contact details on the website will be our setting address, email and telephone number.

87. The administrator account for our website will be secured with an appropriately strong password.

88. We will post appropriate information about safeguarding, including online safety, on our website for members of the School Community.

Publishing Images and Videos Online

89. We will ensure that all images and videos shared online are used in accordance with the associated policies, including, but not limited to, the School's Privacy Notices, Data Protection Policy and Safeguarding Policy.

EMAIL COMMUNICATION

Managing Email

90. Access to our email systems will always take place in accordance with data protection legislation and in line with other policies including, but not limited to, the Behaviour for Learning, Data Protection and Safeguarding policies.

91. The forwarding of any chain messages/emails is not permitted.

92. Spam or junk mail will be blocked and reported to the email provider.

93. Any electronic communication to a non @tiffingirls.org email address which contains sensitive or personal information will only be sent using password protection and/or encryption.

94. School email addresses and other official contact details will not be used for setting up personal social media accounts.

95. Members of the School Community will immediately tell the DSL if they receive offensive communication, and this will be recorded in our safeguarding files/records.

96. Excessive social email use can interfere with teaching and learning and will be restricted; access to external personal email accounts may be blocked on site.

Staff Email

97. The use of personal email addresses by staff for any official School business is not permitted other than in a genuine emergency. All members of staff are provided with an email address to use for all official communication. Staff will sign an acceptable use policy.

98. Staff email communication must adhere to the School's Data Protection policy. Emails created or received will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000, or as part of a Subject Access Request under the UK General Data Protection Regulation. Staff must therefore manage their School email account as directed by the School's Data Protection Officer.

99. Members of staff are encouraged to have an appropriate work life balance when responding to email, especially if communication is taking place between staff, students and parents.

100. If any issues/complaints are involved, then staff sending emails to parents, external organisations or students must follow the protocols set out in the School's Complaints policy.

101. Staff are required to set up the School's standard disclaimer to be attached to all external email correspondence.

Student Email

102. Students will use provided email accounts for educational purposes.

103. Students will sign an acceptable use policy and will receive education regarding safe and appropriate email etiquette before access is permitted.

104. Staff should make students aware of the following:

- They must use appropriate language
- They must not reveal any personal details about themselves or others in email communication
- They must ensure that any email attachments they receive are checked for viruses before opening
- They must immediately inform a member of staff if they receive an offensive email
- They must not forward chain letters – this is not permitted in School

USE OF GOOGLE CLASSROOM, GOOGLE MEET AND/OR USE OF WEBCAMS

105. The School recognises that online learning through Google Meet and the use of webcams can be a challenging activity but brings a wide range of learning benefits.

106. All online learning / Google Meet and webcam equipment will be switched off when not in use.

107. Staff will ensure that online/Google Meet opportunities and/or tools are suitably risk assessed and will ensure that accounts and systems used to access these events are safe and secure.

108. Online learning / Google Meet equipment and webcams will be kept securely and, if necessary, locked away or disabled when not in use.

Users

109. Google Meet will be supervised appropriately, according to the student's age and ability.

110. Google Meet will take place via official and approved communication channels following a robust risk assessment.

111. The unique log on and password details for Google Meet will only be issued to members of staff as part of their school Google account, and should be kept securely, to prevent unauthorised access.

112. When recording a Google Meet lesson, it should be made clear to all parties at the start of the lesson.

113. There are very few occasions where we permit one to one Google meets between staff and students. Such instances are always logged and would have the permission of the DSL or relevant SLT link. On such occasions, one to one Google Meets with students will not be recorded.

114. If third party materials are included, the relevant member of staff will check that recording is permitted to avoid infringing the third-party intellectual property rights and that it is covered by fair use criteria.

115. Students will be regularly advised and reminded of expectations regarding use of camera, blurring of backgrounds, keeping staff informed of Wi-Fi or bandwidth issues and keeping devices fully charged for a day's learning.

MANAGEMENT OF LEARNING PLATFORMS

116. The School uses Google Suite as its official learning platform. Leaders and staff will regularly monitor the usage of the Learning Platform (LP), including message/communication tools and publishing facilities.
Only current members of staff (except Members of the Academy Trust, Governors, Contractors and Visitors), students and parents will have access to the LP. Parents will only have access for specific events such as parents' evenings or focus evenings.

117. When staff and students leave the setting, their account will be disabled or transferred to their new establishment.

118. Students and staff will be advised about acceptable conduct and use when using the LP.

119. All users will be mindful of copyright and will only upload appropriate content onto the LP.

120. Any concerns about content on the LP will be recorded and dealt with in the following ways:
- The user will be asked to remove any material deemed to be inappropriate or offensive
- If the user does not comply, the material will be removed by the site administrator
- Access to the LP for the user may be suspended
- The user will need to discuss the issues with a member of SLT before reinstatement
- A student's parents/carers may be informed
- If the content is illegal, we will respond in line with existing safeguarding procedures

121. Students may require editorial approval from a member of staff. This may be given to the student to fulfil a specific aim and may have a limited time frame.

122. A visitor may be invited onto the LP by a member of SLT and other authorised staff (e.g. Higher Education Programme Coordinator); in this instance, there may be an agreed focus or a limited time slot. Visitors will always be supervised.

Management of Applications (Apps)

123. The Deputy Headteacher will sign off on the use of any Apps or extensions on Chromebooks.

124. The IT Contractor will ensure that the use of tracking systems is appropriately risk assessed prior to use, and that they are used in accordance with data protection legislation, including the General Data Protection Regulation (GDPR).

125. To safeguard students' data

- only student-issued devices will be used for apps that record and store students' personal details, attainment or photographs
- personal staff mobile phones or devices will not be used to access or upload content to any apps which record and store students' personal details, attainment or images unless appropriately encrypted
- devices will be appropriately encrypted if taken off site, to reduce the risk of a data security breach, in the event of loss or theft
- all users will be advised regarding safety measures, such as using strong passwords and logging out of systems
- parents/carers will be informed of the expectations regarding safe and appropriate use, prior to being given access; for example, not sharing passwords or images

SOCIAL MEDIA

General expectations

126. The expectations regarding safe and responsible use of social media apply to all members of the School Community.

127. The term social media may include (but is not limited to): blogs; wikis; social networking sites; forums; bulletin boards; online gaming; apps; video/photo sharing sites; chatrooms and instant messaging.

128. When engaging in social media, all members of the School Community are expected to do so in a positive, safe and responsible manner.

129. All members of the School Community are advised not to publish specific and detailed private thoughts, concerns, pictures or messages on any social media services, especially content that may be considered threatening, hurtful or defamatory to others.

130. The School will control student and staff access to social media whilst using School provided devices and systems on site.

131. Concerns regarding the online conduct of any member of the School Community on social media should be reported to the DSL, Headteacher or Chair of Governors as appropriate, and will be managed in accordance with the relevant School policy e.g. Safeguarding, Managing Allegations of Abuse, Anti-bullying and Behaviour for Learning.

Staff: Personal Use of Social Media

132. Staff are not permitted to access social media websites from School computers/devices at any time unless authorised to do so by a member of SLT (eg for the purposes of the School's online accounts). However, staff may use their own devices to access social media websites while they are in School,

outside of their teaching/working times. Excessive use of social media, which could be considered to interfere with their work, will be considered a disciplinary matter.

133. The safe and responsible use of social networking, social media and personal publishing sites will be discussed with all members of staff as part of staff induction and will be revisited and communicated via regular staff training opportunities.

134. Safe and professional behaviour will be outlined for all members of staff (including volunteers) as part of our Staff Code of Conduct and Acceptable use ICT policy. The 'Teacher's Standards' as published by the Department for Education, expects teachers, in their personal and professional conduct, 'to uphold trust in the profession and maintain high standards of ethics and behaviour, within and outside School'. The School considers this statement to cover the use of social media by ALL staff.

135. All members of staff are advised that their online conduct on social media can have an impact on their role and reputation within the School.

136. Civil, legal or disciplinary action may be taken if staff are found to have brought the profession or institution into disrepute, or if something is felt to have undermined confidence in their professional abilities.

137. All members of staff are advised to safeguard themselves and their privacy when using social media sites. Staff must never give out personal information that identifies their home address, mobile/landline telephone numbers or personal email address.

138. Advice will be provided to staff via staff training and by sharing appropriate guidance and resources on a regular basis. This will include, but is not limited to:

- Setting the privacy levels of their personal sites
- Being aware of location sharing services
- Opting out of public listings on social networking sites
- Logging out of accounts after use
- Keeping passwords safe and confidential
- Ensuring staff do not represent their personal views as that of the School

139. All members of staff are required to carefully consider the information, including text and images, they share and post online and to ensure that their social media use is compatible with their professional role and is in accordance with our policies and the wider professional and legal framework.

140. If a member of staff discovers inappropriate (threatening or malicious) material online concerning themselves or the School, they must: secure and preserve any evidence (e.g. noting a web address, or taking a screenshot) and notify the DSL or the Headteacher who will contact the social network site or internet service provider asking for the material to be removed.

141. Information and content that staff members have access to as part of their employment, including photos and personal information about students and their family members or colleagues must not be shared or discussed on social media sites.

142. Members of staff will notify the DSL and/or the Headteacher immediately if they consider that any content shared on social media sites conflicts with their role.

Staff: Communicating with students and parents/carers

143. Members of staff must not communicate with or add as 'friends' any current students or their family members via any personal social media sites, applications or profiles. Any pre-existing relationships or exceptions that may compromise this, will be discussed with the DSL and/or the Headteacher. In

general, the School suggests that staff avoid communicating with or adding as 'friends' past students or their family members except as set out in the paragraph below.

144. If ongoing contact with students is required once they have left the School, members of staff will be expected to use existing alumnae networks, LinkedIn or use official setting-provided communication tools.

145. Staff will not use personal social media accounts to contact students or parents, nor should any contact be accepted, except in circumstances where prior approval has been given by the DSL and/or the Headteacher.

146. Any communication from students and parents received on a staff member's personal social media accounts must be firmly and politely rejected and must be reported to the DSL and/or The Headteacher.

Staff: Official Use of Social Media

147. The official use of social media as a communication tool has been formally risk assessed and approved by the Headteacher and SLT and the School has official social media accounts. Only social media tools which have been risk assessed and approved as suitable for educational purposes will be used.

148. The official use of social media sites only takes place with clear educational or School Community engagement objectives, with specific intended outcomes.

149. SLT and other relevant staff have access to account information and login details for our social media channels, both for relevant communication and in case of emergency, such as School closure.

150. Staff use the School provided email addresses to register for and manage any official social media channels.

151. Official social media sites are suitably protected and, where possible, linked to our website.

152. Public communications on behalf of the setting will, where possible, be read and agreed by at least one other colleague, but in any event, staff posting on official social media sites will be expected to follow the Staff Code of Conduct.

153. Official social media use will be conducted in line with the School's Privacy Notices and existing policies, including: Anti-bullying, Staff Code of Conduct, Data Protection and Safeguarding.

154. All communication on official social media platforms will be clear, transparent and open to scrutiny.

155. Parents/carers and students will be informed of any official social media use, along with expectations for safe use and action taken to safeguard the School Community. Parental consent will be obtained, as required.

Staff: Expectations for staff using personal social media accounts as part of their capacity as an employee of the School

156. If members of staff are participating in online social media activity as part of their capacity as an employee of the School, they will:

- always be professional and aware they are an ambassador for the School

- make it clear, if disclosing their official role and position, that they do not speak on behalf of the School
- always be responsible, credible, fair and honest, and consider how the information being published could be perceived or shared
- always act within the legal frameworks they would adhere to within the workplace, including: libel, defamation, confidentiality, copyright, data protection and equality laws
- ensure that they have appropriate consent before sharing images on the official social media channel
- not disclose information, make commitments or engage in activities on behalf of the setting, unless they are authorised to do so
- not engage with any direct or private messaging with current students, parents/carers
- inform the DSL and /or member of SLT of any concerns, such as criticism, inappropriate content or contact from students
- not carry out any illegal activity, or activity that could be considered criminal in nature
- Ensure that their use of language, terminology, grammar and spelling reflect the ethos of the school.

Students: Personal Use of Social Media

157. Safe and appropriate use of social media will be taught to students as part of an embedded and progressive education approach, via age appropriate sites and resources.

158. Students will be advised
- To consider the benefits and risks of sharing personal details on social media sites which could identify them and/or their location
- To only approve and invite known friends on social media sites and to deny access to others by making profiles private
- Not to meet any online friends without a parent/carer or other responsible adult's permission and only when a trusted adult is present
- To use safe passwords
- To use social media sites which are appropriate for their age and abilities
- How to block and report unwanted communications
- How to report concerns both within the setting and externally

159. Any concerns regarding a student's use of social media will be dealt with in accordance with existing policies, including Anti-bullying, Behaviour for Learning and Safeguarding. Concerns will be shared with parents/carers as appropriate, particularly when concerning underage use of social media sites, games or tools.

USE OF PERSONAL DEVICES AND MOBILE PHONES

160. The School recognises that personal communication through mobile technologies is an accepted part of everyday life for students, staff and parents/carers, but technologies need to be used safely and appropriately by all members of the school community.

General Expectations

161. All use of personal devices (including but not limited to; tablets, Chromebooks, and 'smart' watches) and mobile phones will take place in accordance with the law and other appropriate policies, such as Staff Code of Conduct, Anti-bullying, Behaviour for Learning and Safeguarding.

162. Electronic devices of any kind that are brought onto site are the responsibility of the user. All members of the School Community are advised to take steps to protect their mobile phones, Chromebooks or devices from loss, theft or damage; the School accepts no responsibility for the loss, theft or damage of such items on our premises.

163. All members of the School Community are advised to use passwords/pin numbers to ensure that unauthorised calls or actions cannot be made on their phones or devices; passwords and pin numbers should be kept confidential and mobile phones and personal devices should not be shared.

164. The sending of abusive or inappropriate messages or content via mobile phones or personal devices is forbidden by any member of the School Community; any breaches will be dealt with as part of our behaviour policy.

165. All members of the School Community are advised to ensure that their mobile phones and personal devices do not contain any content which may be offensive, derogatory or would otherwise contravene our Staff Code of Conduct, Behaviour for Learning or Safeguarding Policies.

Staff use of Personal Devices and Mobile Phones

166. Members of staff will ensure that use of personal phones and devices takes place in accordance with the law, as well as relevant policy and policies, such as: Acceptable Usage, Staff Code of Conduct, Data Protection, Safeguarding and Managing Allegations of Abuse.

167. Staff will be advised to:

- Keep mobile phones and personal devices in a safe and secure place during lesson time
- Keep mobile phones and personal devices switched off or switched to 'silent' mode during lesson times
- Ensure that Bluetooth or other forms of communication (such as 'airdrop') are hidden or disabled during lesson times
- Not use personal devices during teaching periods, unless permission has been given by the Headteacher, such as in emergency circumstances or where a second device is needed for work purposes
- Ensure that any content brought onto site via mobile phones and personal devices are compatible with their professional role and expectations

168. Members of staff are not permitted to use their own personal phones or devices for contacting students or parents/carers. Any pre-existing relationships which could undermine this will be discussed with the Headteacher.

169. Staff will not use personal devices:

- to take photos or videos of students unless express permission has been given by the Headteacher or SLT link e.g. in order to upload an image to one of the school's social media accounts (see Photographs and Images Policy). Any photo taken by an authorised member of staff on a personal device must be deleted after use (including from any cloud storage) and can only be taken, transmitted or published with the person's permission
- directly with students and will only use work-provided equipment during lessons/educational activities

170. If a member of staff breaches this policy, action will be taken in line with the School's Disciplinary policy.

171. If a member of staff is thought to have illegal content saved or stored on a mobile phone or personal device or to have committed a criminal offence, the police will be contacted.

172. When working remotely (e.g. during a period of local or national lockdown), staff may use personal devices, but still following the guidance and directives set out in this online safety policy, and the School's Acceptable Use policy. Specific guidance will be issued as needed in the event of an extended school closure.

Students' Use of Personal Devices and Mobile Phones

173. Mobile phones or personal devices are not be used by students (Yr7-11) on the school site.

174. We will comply with our other legal duties such as the duty to make reasonable adjustments where necessary for example to allow students to use smart technology to meet their medical needs. These arrangements must be agreed with the Head of Year / SENCO in advance.

175. Students in Year 11 are allowed to use their Chromebooks at break and lunchtime for school work. Years 7 – 10 may not use their Chromebooks at these times, unless they are participating in an online club and have been given special permission.

176. Students in Years 12-13 are allowed to use their mobile phones or other personal devices while in the Sixth Form Centre.

177. Use of mobile phones on school trips:

- The general rule is that mobile phone use on trips is the same as in school
- We understand that students will want to bring mobile phones on trips and activities; however, they must remain turned off and not used unless there is specific time limited permission given by a member of staff following clear guidance as to how they can be used. For example, to contact parents when students return from the trip
- Students will be able to use phones for medical needs as agreed in advance by their family, the Trip Leader and HOY (e.g. the diabetes app).
- If it is agreed photographs can be taken on the trip it must be with a standard camera should be used rather than a smart device
- No pictures should be taken of any staff/volunteers with any device
- Images must not be posted online including social media, WhatsApp and other messaging services
- The school accepts no responsibility for the loss, theft or damage of mobile phones or other hardware

- Any breaches of these expectations will lead to the phone being confiscated for the rest of the day (in line with the school behaviour policy). You will have the phone returned to them the next day.

178. Students will be educated regarding the safe and appropriate use of personal devices and mobile phones and will be made aware of boundaries and consequences.

179. Mobile phones and personal devices must not be taken into examinations. Students found in possession of a mobile phone or personal device during an exam will be reported to the appropriate examining body. This may result in the withdrawal from either that examination or all examinations.

180. If a student breaches the policy, sanctions and interventions will be applied in accordance with the Behaviour for Learning Policy and/or the Discrimination Incident policy where relevant.

181. Staff may confiscate a student's mobile phone or device if they believe it is being used to contravene the School's Behaviour for Learning or Anti-Bullying Policy. The following would apply:

- Searches of mobile phone or personal devices will only be carried out in accordance with our Behaviour for Learning and Safeguarding Policies and in accordance with Department for Education advice on 'Searching, Screening and Confiscation' as issued from time to time.
- The headteacher, and any member of staff authorised to do so by the headteacher as set out in our behaviour policy, can carry out a search and confiscate any electronic device that they have reasonable grounds for suspecting:
  - Poses a risk to staff or students, and/or
  - Is identified in the school rules as a banned item for which a search can be carried out, and/or
  - Is evidence in relation to an offence
- Before a search, if the authorised staff member is satisfied that they have reasonable grounds for suspecting any of the above, they will also:
  - Make an assessment of how urgent the search is and consider the risk to other students and staff.
  - If the search is not urgent, they will seek advice from the headteacher /DSL
  - Explain to the student why they are being searched, and how the search will happen; and give them the opportunity to ask questions about it
  - Seek the student's co-operation
- Authorised staff members may examine, and in exceptional circumstances erase, any data or files on an electronic device that they have confiscated where they believe there is a 'good reason' to do so.
- When deciding whether there is a 'good reason' to examine data or files on an electronic device, the staff member should reasonably suspect that the device has, or could be used to:
  - Cause harm, and/or
  - Undermine the safe environment of the school or disrupt teaching, and/or
  - Commit an offence
- If inappropriate material is found on the device, it is up to the staff member in conjunction with the DSL / headteacher / other member of the senior leadership team to decide on a suitable response. If there are images, data or files on the device that staff reasonably suspect are likely to put a person at risk, they will first consider the appropriate safeguarding response.
- When deciding whether there is a good reason to erase data or files from a device, staff members will consider if the material may constitute evidence relating to a suspected offence. In these instances, they will not delete the material, and the device will be handed to the police as soon as reasonably practicable. If the material is not suspected to be evidence in relation to an offence, staff members may delete it if:
  - They reasonably suspect that its continued existence is likely to cause harm to any person, and/or
  - The student and/or the parent/carer refuses to delete the material themselves
- If a staff member **suspects** a device **may** contain an indecent image of a child (also known as a nude or semi-nude image), they will:
  - **Not** view the image
  - Confiscate the device and report the incident to the DSL (or equivalent) immediately, who will decide what to do next. The DSL will make the decision in line with the DfE's latest guidance on screening, searching and confiscation and the UK Council for Internet Safety (UKCIS) guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people
- Any searching of students will be carried out in line with:
  - The DfE's latest guidance on searching, screening and confiscation
  - UKCIS guidance on sharing nudes and semi-nudes: advice for education settings working with children and young people

        - Our behaviour policy
    - Any complaints about searching for or deleting inappropriate images or files on students' electronic devices will be dealt with through the school complaints procedure. Mobile phones and devices that have been confiscated will be released to students at the end of the school day, or to parents/carers in cases of repeated breaches of the Behaviour for Learning policy.
    - If there is suspicion that material on a student's personal device or mobile phone may be illegal or may provide evidence relating to a criminal offence, the device will be handed over to the police for further investigation

182. Where students' mobile phones or personal devices are used when learning at home, such as in response to local or full lockdowns, this will be in accordance with our Acceptable Use Policy.

Visitors' Use of Personal Devices and Mobile Phones

183. Parents/carers and visitors (including volunteers and contractors) must use their mobile phones and personal devices in accordance with our acceptable use policy and other associated policies, such as: Anti-bullying, Behaviour for Learning and Safeguarding.

184. We will ensure appropriate signage and information is displayed and provided to inform parents, carers and visitors of expectations of use.

185. Members of staff are expected to challenge visitors if they have concerns and will always inform the DSL.

Officially Provided Mobile Phones and Devices

186. Members of staff may be issued with a work phone number, where contact with students or parents/carers is required (e.g. site team). In addition, occasionally School provided mobile phones/devices will be issued to staff where appropriate.

187. School mobile phones and devices will be suitably protected via a passcode/password/pin and must only be accessed or used by members of staff.

188. School mobile phones and devices will always be used in accordance with the relevant policies.

RESPONDING TO ONLINE SAFETY INCIDENTS AND CONCERNS

189. All members of the School Community will be made aware of the reporting procedure for online safety concerns, including: breaches of filtering, youth produced sexual imagery (sexting), online bullying and illegal content.

190. All members of the School Community must respect confidentiality and the need to follow the official procedures for reporting concerns. Students, parents and staff will be informed of the School's Complaints procedure and staff are made aware of the Whistleblowing procedure.

191. The School requires staff, parents/carers and students to work in partnership to resolve online safety issues. After any investigations are completed, the DSL will debrief, identify lessons learnt and implement any policy or curriculum changes as required.

192. If the School is unsure how to proceed with an incident or concern relating to adult misconduct, the DSL will seek advice from the Local Authority Designated Officer (LADO).

193. Where there is suspicion that illegal activity has taken place, the DSL will contact the LADO or Police as appropriate using 101, or 999 if there is immediate danger or risk of harm.

194. If an incident or concern needs to be passed beyond our School Community (for example if other local Schools are involved or the public may be at risk), the DSL will speak with the police and/or the LADO first to ensure that potential investigations are not compromised.

Concerns about student welfare

195. The DSL will be informed of any online safety incidents involving Safeguarding concerns.

196. The DSL will record these issues in line with our Safeguarding and Child Protection policies.

197. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with appropriate thresholds and procedures.

198. The DSL and/or Headteacher will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

199. Any complaint about staff misuse will be referred to the DSL and/or Headteacher (or to the Chair of the Governing Board if the complaint is about the Headteacher's misuse).

200. Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO) in accordance with the relevant School policy including, but not limited to, Disciplinary, Safeguarding and/or Allegations of Abuse policies.

201. Appropriate action will be taken in accordance with our Safeguarding, Managing Allegations of Abuse, Disciplinary and/or Safeguarding policies.

PROCEDURES FOR RESPONDING TO SPECIFIC ONLINE INCIDENTS OR CONCERNS

Online Sexual Violence and Sexual Harassment Between Children

202. The School has accessed and understood Department for Education advice: Sexual violence and sexual harassment between children in Schools and colleges, and relevant sections of statutory guidance covering online safety in 'Keeping Children Safe in Education'.

203. The School recognises that sexual violence and sexual harassment between children can take place online. Examples may include; non-consensual sharing of sexual images and videos, sexualised online bullying, online coercion and threats, unwanted sexual comments and messages on social media, and online sexual exploitation. Full details of how we will respond to concerns relating to sexual violence and sexual harassment between children can be found within our Behaviour for Learning, Discrimination Incident, Safeguarding and Anti-bullying Policies.

204. The School recognises that the internet brings the potential for the impact of any sexual violence and sexual harassment concerns to extend further than the local community, and for a victim or alleged perpetrator to become marginalised and excluded by online communities.

205. The School also recognises the potential for repeat victimisation in the future if abusive content continues to exist somewhere online.

206. The School will ensure that all members of the School Community are made aware of the potential social, psychological and criminal consequences of online sexual violence and sexual harassment between children by implementing a range of age and ability appropriate educational methods as part of our PSHE and RSHE curriculum.

207. The School will ensure that all members of the School Community are aware of sources of support regarding online sexual violence and sexual harassment between children.

208. The School will respond to concerns regarding online sexual violence and sexual harassment between children, regardless of whether the incident took place on our premises or using our equipment.

209. If made aware of online sexual violence and sexual harassment, the School will:

- Immediately notify the DSL and Headteacher and act in accordance with our Behaviour for Learning, Discrimination Incident, Safeguarding and Anti-bullying Policies
- If content is contained on students' electronic devices, they will be managed in accordance with the Department for Education's advice on 'searching screening and confiscation'.
- Provide the necessary safeguards and support for all students involved, such as offering specific advice on blocking, reporting and removing online content, as well as providing appropriate counselling/pastoral support
- Implement appropriate sanctions in accordance with our Behaviour for Learning policy
- Inform parents/carers, if appropriate, about the incident and how it is being managed
- If appropriate, make a referral to partner agencies, such as Children's Social Services and/or the Police
- If the concern involves children and young people at a different educational setting, work in partnership with other DSLs to ensure appropriate safeguarding action is taken in the wider local community
- If a criminal offence has been committed, the DSL will discuss this with the police first to ensure that investigations are not compromised
- Review the handling of any incidents to ensure that best practice was implemented, and policies/procedures are appropriate

Youth Produced Sexual Imagery

210. The School recognises consensual and non-consensual sharing of nude and semi-nude images and/or videos (known as youth produced sexual imagery or known as "sexting") is a safeguarding issue; all concerns will be reported to and dealt with by the DSL.

211. The School will follow the advice as set out in KCSIE.

212. The School will ensure that all members of the School Community are made aware of the potential social, psychological and criminal consequences of consensual and non-consensual sharing of nude and semi-nude images and/or videos by implementing preventative approaches, via a range of age and ability appropriate educational methods.

213. The School will ensure that all members of the School Community are aware of sources of support regarding consensual and non-consensual sharing of nude and semi-nude images and/or videos .

214. The School will respond to concerns regarding youth produced sexual imagery, regardless of whether the incident took place on site or using School provided or personal equipment.

215. The School will not:

- view any images suspected of being youth produced sexual imagery, unless there is no other possible option, or there is a clear need or reason to do so - If it is deemed necessary, the image

will only be viewed by the DSL and their justification for viewing the image will be clearly documented
- send, share, save or make copies of content suspected to be an indecent image of a child (i.e. youth produced sexual imagery) and will not allow or request students to do so

216. If made aware of an incident involving the creation or distribution of consensual and non-consensual sharing of nude and semi-nude images and/or videos, the School will:
- act in accordance with our safeguarding and child protection policies and the relevant safeguarding procedures
- ensure the DSL responds in line with the KCSIE guidance
- store the device securely
- if an indecent image has been taken or shared on our network or devices, act to block access to all users and isolate the image
- carry out a risk assessment which considers any vulnerability of students involved; including carrying out relevant checks with other agencies
- inform parents/carers, if appropriate, about the incident and how it is being managed
- make a referral to Children's Social Services and/or the Police, as deemed appropriate in line with KCSIE guidance
- provide the necessary safeguards and support for students, such as offering counselling or pastoral support
- implement appropriate sanctions in accordance with our Behaviour for Learning policy but taking care not to further traumatise victims where possible
- consider the deletion of images in accordance with the KCSIE guidance
- delete images only when the DSL has confirmed that other agencies do not need to be involved; and are sure that to do so would not place a child at risk or compromise an investigation
- review the handling of any incidents to ensure that best practice was implemented; SLT will also review and update any management procedures, where necessary

Incidents involving Safeguarding concerns

217. The DSL will record these issues in line with the School's Safeguarding policy.

218. The DSL will ensure that online safety concerns are escalated and reported to relevant agencies in line with the safeguarding procedures.

219. The DSL and/or Headteacher will inform parents/carers of online safety incidents or concerns involving their child, as and when required.

Staff Misuse

220. Any complaint about staff misuse will be referred to the DSL and/or the Headteacher.

221. Any allegations regarding a member of staff's online conduct will be discussed with the Local Authority Designated Officer (LADO).

222. Appropriate action, where relevant, will be taken in accordance with our Safeguarding, Managing Allegations of Abuse and/or Disciplinary policies.

ARTIFICIAL INTELLIGENCE (AI)

223. Generative artificial intelligence (AI) tools are now widespread and easy to access. Staff, students and parents/carers may be familiar with generative chatbots such as ChatGPT and Google Bard.

224. As outlined in the AI Policy :

- there are mechanisms for ongoing monitoring and evaluation of AI applications to ensure alignment with the school's goals and ethical standards. Regular reviews and updates to the AI policy will be conducted.
- Staff should be aware of the risks of using AI tools whilst they are still being developed and should carry out a risk assessment where new AI tools are being used by the school (refer to the AI Policy).
- Any use of AI must also conform to our GDPR policies. No data or personal information relating to students, families or staff should be uploaded into an AI platform.

225. The school has chosen to allow students access to Google Gemini and Gemini Teens, which is ring fenced within Google Workspace for Education. It will share GDPR and Safeguarding information relating to this platform with all stakeholders.

226. The School recognises that AI has many uses to help students learn, but may also have the potential to be used to bully others. For example, in the form of 'deepfakes', where AI is used to create images, audio or video hoaxes that look real. This includes deepfake pornography: pornographic content created using AI to include someone's likeness. The School will treat any use of AI to bully students in line with our anti-bullying and behaviour policy. Creating or sharing deepfake pornography of someone without their permission is a new criminal offence under the Online Safety Act 2023 and any incidents will be shared with the Police and other relevant authorities.

ONLINE SAFETY LINKS AND CONTACTS

Child Exploitation and Online Protection (CEOP)	www.ceop.police.uk www.thinkuknow.co.uk
Childnet	www.childnet.com
NSPCC	www.nspcc.org.uk/onlinesafety
Childline	www.childline.org.uk
UK Safer Internet Centre	www.saferinternet.org.uk
Internet Watch Foundation	www.iwf.org.uk
Internet Matters	www.internetmatters.org
Net Aware	www.net-aware.org.uk