

Online Safety Policy

17 October 2026

About This Document

Annual Policy Period	2025 - 2026
Policy Adopted by Governors	September 2019
Last Policy Review	8 October 2026
Next Policy Review	September 2027

History

Version	Date	Name	Description
0.1	Sep 2019	René Esterhuizen, Clerk to Trustees	First release. DRAFT
1.0	Sep 2019	School Governors	Approved and adopted.
1.1	Mar 2021	School Governors	Reviewed and approved.
1.2	1 Sep 2021	School Governors	Reviewed and approved.
1.3	1 Sep 2022	School Governors	Reviewed and approved.
1.4	13 Sep 2023	School Governors	Reviewed and approved.
1.5	16 May 2024	School Governors	Reviewed and approved.
1.6	30 Aug 2024	School Governors	Reviewed and approved.
1.7	13 Sep 2025	René Esterhuizen, Headteacher	Reviewed, no changes.
1.8	7 Oct 2026	René Esterhuizen, Headteacher	Reviewed, updated to come in line with new KCSIE guidelines.
1.9	17 Oct 2026	Dave Walker	Change of personnel para 27.3

Contents

1. Introduction 4
2. Data Protection 6
3. Disinformation, Misinformation, And Harmful Content 6
4. Cybercrime 6
5. Online Safety: Filtering,Monitoring and AI-Related Risks 6
6. Breaches 7
7. Incident Reporting 7
8. Computer Viruses 8
9. Data Security 8
10. Security 8
11. Information Asset Owner (IAO) 9
12. Disposal of Redundant ICT Equipment Policy 9
13. Online/Virtual Teaching 10
14. Email 11
15. Equal Opportunities: Students with Additional Needs 14
16. Online Safety Roles and Responsibilities 14
17. Online Safety in the Curriculum 14
18. Online Safety Skills Development for Staff 15
19. Managing the School Online Safety Messages 15
20. Incident Reporting, Online Safety & Infringements 15
21. Internet Access 16
22. Managing Other Online Technologies 17
23. Parental Involvement 18
24. Passwords and Password Security 18
25. Personal or Sensitive Information 20
26. Remote Access 20
27. Safe Use of Images 21
28. School ICT Equipment 23
29. Social media 26
30. Servers 26
31. Systems and Access 27

1. Introduction

1.1. This policy applies to this independent school and should be read alongside the Safeguarding and Child Protection Policy, Behaviour Policy, Data Protection Policy, Acceptable Use Agreements and mobile-phone arrangements. It has regard to KCSIE 2026; the Education (Independent School Standards) Regulations 2014; the Data Protection Act 2018, UK GDPR and Data (Use and Access) Act 2025; the Equality Act 2010; the Human rights Act 1998; the Computer Misuse Act 1990; the Copyright, Designs and Patents Act 1988; the Online Safety Act 2023; the Prevent duty guidance 2023; DfE filtering and monitoring standards updated in 2026; and the statutory Mobile phones in schools guidance applying from 1 September 2026.

i. Data Protection

ii. Keeping Children Safe in Education 2026

1.2. At The Vine Christian School, we understand the responsibility to educate our students on online safety issues. Teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

1.3. Online safety is a key part of safeguarding so that young people do not see the internet as a separate part of their lives. The school will ensure that online safety is delivered as part of the curriculum on a regular basis.

1.4. We understand that the breadth of online safety issues is considerable and continually evolving. In line with KCSIE 2026, the school considers the four areas of online risk: content, contact, conduct and commerce, including risks arising from generative artificial intelligence, deepfakes, impersonation, algorithmic systems, misinformation and disinformation.

i. **content:** being exposed to illegal, inappropriate, or harmful content, for example: pornography, fake news, racism, misogyny, self-harm, suicide, anti-Semitism, radicalisation, and extremism, extreme sexual or physical violence.

ii. **contact:** being subjected to harmful online interaction with other users or generative AI applications that simulate this. 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.

iii. **conduct:** online behaviour that increases the likelihood of, or causes, harm; for example, making, sending, and receiving explicit images, including those generated using AI, consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying, and

iv. **commerce:** risks such as online gambling, inappropriate advertising, phishing and or financial scams. If we feel any of our pupils, or staff are at risk, it will be reported to the Anti-Phishing Working Group.

1.5. Internet, mobile and digital technologies in the 21st century are essential resources to support learning and teaching, as well as playing an important role in the everyday lives of children, young people, and adults. Consequently, schools need to build in the use of these technologies to arm our young people with the skills to access life-long learning and employment.

1.6. Internet, mobile and digital technologies cover a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of internet, mobile and digital technologies within our society. Currently the internet technologies children and young people are using include:

i. Websites.

ii. Apps.

iii. Email, Instant Messaging, and chat rooms.

iv. Social Media, platforms and services.

v. Mobile/ Smart phones with text, video and/ or web functionality.

vi. Other mobile devices including tablets and gaming devices.

vii. Online Games.

viii. School-approved learning platforms and online learning services.

ix. Learning Platforms and Virtual Learning Environments.

x. Blogs and Wikis.

xi. Podcasting.

xii. Video sharing.

xiii. Downloading.

xiv. On demand TV and video, movies, radio and Smart TVs.

1.7. Whilst exciting and beneficial both in and out of the context of education, much internet, mobile and digital technologies, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these technologies and that individual online services may have minimum-age requirements.

1.8. Schools hold personal data on learners, staff, and others to help them conduct their day-to-day activities. Some of this information is sensitive and could be used by another person or criminal organisation to cause harm or distress to an individual. The loss of sensitive information can result in media coverage and potentially damage the reputation of the school. This can make it more difficult for your school to use technology to benefit learners.

1.9. Everybody in the school community has a shared responsibility to secure any sensitive information used in their day-to-day professional duties and even staff not directly involved in data handling should be made aware of the risks and threats and how to minimise them.

1.10. Both this policy and the Acceptable Use Agreement (for all staff, Trustees and Governors, regular visitors [for regulated activities] and students) are inclusive of both fixed and mobile internet; technologies provided by the school (such as laptops, mobile devices, webcams, whiteboards, digital video equipment, etc.); and technologies owned by students and staff, but brought onto school premises (such as laptops, mobile phones, and other mobile devices).

2. Data Protection

2.1. The Vine Christian School holds a separate Data Protection Policy, including UK GDPR.

3. Disinformation, Misinformation, And Harmful Content

3.1. Pupils may be exposed to false or misleading content online, including conspiracy theories, political misinformation, health-related disinformation, or extremist narratives. The school recognises this as a safeguarding risk. Staff will be trained to identify signs that a pupil may be affected by such content and respond appropriately. Digital literacy and critical thinking are embedded in the curriculum to help children challenge and question information responsibly. Where such exposure presents a risk of radicalisation or emotional harm, staff will follow safeguarding and Prevent referral procedures.

4. Cybercrime

4.1. Cybercrime is criminal activity committed using computers and/or the internet. It may be cyber-enabled, where technology increases the scale or speed of an offence that could also occur offline, or cyber-dependent, where the offence can only be committed using a computer or network.

4.2. Cyber-dependent offences may include unauthorised access to computers or networks, denial-of-service attacks, and creating, supplying or obtaining malware or other tools for use in cybercrime. Staff should be aware that children with particular skills or interests in computing and technology may become involved in illegal activity without fully understanding the legal, ethical or safeguarding implications.

4.3. Any concerns about a pupil becoming involved in cybercrime should be reported to the Designated Safeguarding Lead or deputy. Where appropriate, the DSL should consider referral to the Cyber Choices programme, a preventative police programme which aims to divert young people who are at risk of becoming involved in low-level cyber-dependent offending towards positive uses of their skills and interests. Normal safeguarding procedures should also be followed where there are concerns about exploitation, coercion or harm.

5. Online Safety: Filtering, Monitoring and AI-Related Risks

5.1. The school uses appropriate filtering and monitoring systems to protect pupils from illegal, inappropriate and harmful online content. In line with KCSIE 2026 and the DfE Filtering and Monitoring core standard updated in 2026, roles and responsibilities are clearly assigned, safeguarding alerts are acted upon promptly, and provision is reviewed at least once every academic year by the SLT member responsible for filtering and monitoring, with the support of the DSL and IT support. Reviews will include checks that filtering is working appropriately on all internet-connected devices in all relevant locations, and a record will be kept of these checks. The review will consider whether systems can respond appropriately to dynamic, personalised and AI-generated content.

5.2. Appropriate filtering and monitoring technology on school devices and school networks form part of our online safety. We ensure we have effective monitoring strategies in place that meet our safeguarding needs.

5.3. Our school's filtering and monitoring technology is the responsibility of the Designated Safeguarding Lead.

5.4. IT use is monitored using the following filtering and monitoring system: Smoothwall.

5.5. The school will review its overall approach to online safety at least annually, including filtering and monitoring provision. This review will be supported by an annual risk assessment which considers and reflects the online risks faced by the school's pupils, including emerging risks associated with new technologies and generative AI.

5.6. The school will block harmful and inappropriate content without unreasonably impacting teaching and learning.

5.7. Our governing body/trustees review/s the standards and discusses with IT staff and service providers what more needs to be done to support the school in meeting this standard.

5.8. Monitoring, interception and access to communications will be lawful, necessary, proportionate and transparent, and will comply with current data protection law, the Human Rights Act 1998 and applicable communications legislation, including the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 where relevant. Monitoring will be undertaken only for legitimate school purposes and with appropriate governance and safeguards.

5.9. Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

6. Breaches

6.1. A breach or suspected breach of policy by a school employee, contractor or student may result in the temporary or permanent withdrawal of school ICT hardware, software, or services from the offending individual.

6.2. For staff, any policy breach is grounds for disciplinary action in accordance with the school Disciplinary Procedure or, for Support Staff, in their Probationary Period as stated.

6.3. Policy breaches may also lead to criminal or civil proceedings.

6.4. The Information Commissioner has regulatory and enforcement powers under current data protection law. The school will manage personal-data breaches and regulatory obligations in accordance with its Data Protection Policy and current ICO guidance.

6.5. For students, reference will be made to the school's behaviour policy.

7. Incident Reporting

7.1. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of internet, mobile and digital technologies must be immediately reported to the school's relevant responsible person. Additionally, all security breaches, lost/stolen equipment, or data (including remote-access credentials and authentication information), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the relevant responsible person. The relevant responsible individuals in the school are as follows: Mrs. René Esterhuizen and Mr. David Walker.

7.2. Please refer to the relevant section on Incident Reporting, online safety Incident Log & Infringements.

8. Computer Viruses

8.1. All files downloaded from the Internet, received via email or on removable media such as a USB storage device or other removal media must be checked for any viruses using school provided security or endpoint-protection before being used.

8.2. Never interfere with any anti-virus software installed on school ICT equipment.

8.3. If a machine is not routinely connected to the school network, provision must be made for regular security updates through the IT team.

8.4. If a virus is suspected on any school ICT equipment, the use of the equipment must be stopped and the ICT support provider contacted immediately. The ICT support provider will advise on what actions to take and be responsible for advising others that need to know.

9. Data Security

9.1. The accessing and appropriate use of school data is something that the school takes very seriously.

9.2. Security of Confidential and Personal Data - Electronic and Paper:

i. It is critical that the school considers the safety of confidential / personal data removed from a school site (electronic and paper).

ii. We will ensure that ALL staff are aware of how to handle sensitive or personal information.

iii. USB storage devices or other removable media are best encrypted in their entirety.

iv. Staff laptops that hold personal data should have an encrypted 'container' created where all sensitive data should be stored.

v. Backup media must always be kept secure.

10. Security

10.1. The school gives relevant staff access to its Management Information System, with a unique username and password.

10.2. It is the responsibility of everyone to keep passwords secure.

10.3. Staff are aware of their responsibility when accessing school data.

10.4. Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.

10.5. Staff keep all school related data secure. This includes all personal, sensitive, confidential, or classified data.

10.6. Staff should avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, keep it locked out of sight.

10.7. Staff should always carry portable and mobile ICT equipment or removable media as hand luggage and always keep it under your control.

10.8. It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential, and classified information contained in documents copied, scanned, or printed. This is particularly important when shared copiers (multi-function print, scan, and copiers) are used.

11. Information Asset Owner (IAO)

11.1. Any information that is sensitive needs to be protected. This will include the personal data of learners and staff, such as assessment records, medical information, and special educational needs data.

11.2. A responsible member of staff should be able to identify across the school:

i. what information is held, and for what purposes.

ii. what information needs to be protected, how information will be amended or added to over time.

iii. who has access to the data and why?

iv. how information is retained and disposed of.

v. can manage and address risks to the information and make sure that information handling complies with legal requirements. In a Secondary School, there may be several individuals, whose roles involve such responsibility.

vi. However, it should be clear to all staff that the handling of secured data is everyone's responsibility – whether they are an employee, consultant, software provider or managed service provider. Failing to apply appropriate controls to secure data could amount to gross misconduct or even legal action.

vii. The IAO in this school is Mrs. René Esterhuizen

12. Disposal of Redundant ICT Equipment Policy

12.1. All redundant ICT equipment will be disposed of through an authorised agency. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data.

12.2. An appropriate secure data-erasure method will be used for all redundant ICT equipment that may have held personal data to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed. We will only use authorised companies who will supply a written guarantee that this will happen.

12.3. Disposal of any ICT equipment will conform to:

i. The Waste Electrical and Electronic Equipment Regulations 2013

ii. Data Protection Act 2018

- https://www.legislation.gov.uk/ukpga/2018/12/contents

12.4. The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal.

12.5. The school's disposal record will include:

i. Date item disposed of.

ii. Authorisation for disposal.

iii. Verification of software licensing.

iv. Any personal data.

v. How it was disposed of e.g., waste, gift, sale.

vi. Name of person and/or organisation who received the disposed item.

vii. If personal data is likely to have been held on any storage media an appropriate secure data-erasure method will be used to ensure the data is irretrievably destroyed.

viii. Any redundant ICT equipment being considered for sale/gift will have been subject to a recent electrical safety check and hold a valid PAT certificate.

12.6. Further information available at:

i. Waste Electrical and Electronic Equipment (WEEE) Regulations

ii. The Waste Electrical and Electronic Equipment Regulations 2013

iii. https://www.legislation.gov.uk/uksi/2013/3113/contentsInformation Commissioner Website

- https://ico.org.uk/

iv. Data Protection Act – data protection guide

https://www.legislation.gov.uk/ukpga/2018/12/contents

13. Online/Virtual Teaching

13.1. If the school needs to use online or virtual teaching the school will:

i. Ensure all relevant staff are briefed so they understand the policies and the standards of conduct expected of them.

ii. Set clearly defined operating times for virtual learning.

iii. Consider the impact that virtual teaching may have on children and their parents/carers/siblings.

iv. Determine whether there are alternatives to virtual teaching in 'real-time' – e.g., using audio only, pre-recorded lessons, existing online resources.

v. Ensure senior staff and DSL are able to drop into any virtual lesson at any time – the online version of entering a classroom; therefore, the school will make these people aware of the virtual learning timetable and ensure they have the capacity to join a range of lessons.

vi. Take into account any advice published by the local authority, of their online safety/monitoring software provider.

vii. Be in regular contact with parents and carers. These communications will be used to reinforce the importance of children being safe online.

viii. Make it clear to parents and carers the system the school uses to filter and monitor online use.

ix. Make sure parents and carers are aware of what their children are being asked to do online, including the sites they will be asked to access and be clear who from the school (if anyone) their child is going to be interacting with online.

13.2. Whilst using online or virtual teaching staff should:

i. Adhere to their establishment's policy on using online or virtual teaching as laid out here.

ii. Be appropriately dressed.

iii. Think about the background; photos, artwork, identifying features, mirrors – ideally the backing should be nondescript.

iv. Ensure staff and pupils are in living/communal areas – no bedrooms.

v. Ensure all resources/DVDs are age appropriate.

vi. Ensure that the headteacher is aware that the online lesson/meeting is taking place and for what purpose.

vii. Avoid one to one situations – request that a parent is present in the room for the duration or ask a colleague or member of the SLT to join the session.

viii. Only record lessons or online meetings with a pupil where this has been agreed with the headteacher or other senior staff, and the pupil and their parent/carer have given explicit written consent to do so.

ix. Be able to justify images of pupils in their possession.

13.3. This means that adults should not:

i. contact pupils outside the operating times defined by the headteacher.

ii. take or record images of pupils for their personal use.

iii. record virtual lessons or meetings using personal equipment (unless agreed and risk assessed by senior staff).

iv. engage online while children are in a state of undress or semi-undress.

13.4. It is the responsibility of the staff member to act as a moderator; raise any issues of suitability (of dress, setting, behaviour) with the child and/or parent immediately and end the online interaction if necessary.

13.5. Recording lessons does not prevent abuse. If staff wish to record the lesson they are teaching, consideration should be given to data protection issues, e.g., whether parental/pupil consent is needed and retention/storage.

13.6. If a staff member believes that a child or parent is recording the interaction, the lesson should be brought to an end or that child should be logged out immediately.

13.7. Staff, parents and pupils should be aware of the standards of conduct required.

13.8. If staff need to contact a pupil or parent by phone and do not have access to a work phone, they should discuss this with the headteacher and, if there is no alternative, always use 'caller withheld' to ensure the pupil/parent is not able to identify the staff member's personal contact details.

14. Email

14.1. The use of email within most schools is an essential means of communication for both staff and students. In the context of school, email should not be considered private. Educationally, email can

offer significant benefits including direct written contact between schools on different projects, be they staff based or student based, within school or international. We recognise that students need to understand how to style an email in relation to their age and how to behave responsible online.

14.2. Managing Email:

i. The school gives all staff, trustees, and governors their own email account to use for all school business as a work-based tool. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.

ii. Staff, trustees, and governors should use their school email for all professional communication.

iii. It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged, if necessary, email histories can be traced. The school email account should be the account that is used for all school business.

iv. Under no circumstances should staff contact students, parents or conduct any school business using personal email addresses.

v. The school requires a standard disclaimer to be attached to all email correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder.

vi. All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.

vii. Staff sending emails to external organisations, parents or students are advised to cc. the headteacher.

viii. Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.

ix. Emails created or received as part of school business are school records and must be managed in accordance with the school's Data Protection Policy and records-retention arrangements. Staff must therefore actively manage their own e-mail accounts. as follows:

- Delete all emails of short-term value.
- Organise email into folders and carry out frequent housekeeping on all folders and archives.

x. All student email users are expected to adhere to the generally accepted rules of responsible online behaviour particularly in relation to the use of appropriate language and not revealing any personal details about themselves or others in email communication, or arrange to meet anyone without specific permission, virus checking attachments.

xi. Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting email.

xii. Staff must inform (the online safety coordinator or Headteacher) if they receive an offensive e-mail.

xiii. Students are introduced to email as part of the Computing Programme of Study.

xiv. In whatever way you access your school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

14.3. Sending Emails:

i. If sending emails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section:
    - Emailing Personal, Sensitive, Confidential or Classified Information.

ii. Use your own school email account so that you are clearly identified as the originator of a message.

iii. Keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.

iv. Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

v. School email is not to be used for personal advertising.

14.4. Receiving Emails:

i. Check your emails regularly.

ii. Activate your 'out-of-office' notification when away for extended periods.

iii. Never open attachments from an untrusted source.

iv. Do not use the email systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.

v. The automatic forwarding and deletion of emails is not allowed.

14.5. Emailing Personal, Sensitive, Confidential or Classified Information:

i. Where your conclusion is that an email must be used to transmit such data, obtain express consent from your Headteacher to provide the information by email and exercise caution when sending the email. Always follow these checks before releasing the email:
    - Encrypt and password protect.
    - Verify the details, including accurate email address, of any intended recipient of the information.
    - Verify (by phoning) the details of a requestor before responding to email requests for information.
    - Do not copy or forward the email to any more recipients than is necessary.
    - Do not send the information to any person whose details you have been unable to separately verify (usually by phone).
    - Send the information as an encrypted document **attached** to an email.
    - Provide the encryption key or password by a **separate** contact with the recipient(s).
    - Do not identify such information in the subject line of any email.
    - Request confirmation of safe receipt.

15. Equal Opportunities: Students with Additional Needs

15.1. The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the schools' online safety rules.

15.2. However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of online safety issues.

15.3. Where a pupil has poor social understanding, careful consideration should be given to group interactions when raising awareness of online safety. Internet activities should be planned and well managed for these children and young people.

16. Online Safety Roles and Responsibilities

16.1. As online safety is an important aspect of strategic leadership within the school, the Headteacher and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

16.2. The named online safety Safeguarding Officer in this school is Mrs. René Esterhuizen who has been designated this role as a member of the senior leadership team. All members of the school community have been made aware of who holds this post.

16.3. It is the role of the online safety Safeguarding Officer to keep abreast of current issues and guidance through organisations such as the LEA, CEOP (Child Exploitation and Online Protection) and Childnet.

16.4. Senior Management and Trustees are updated by the online safety Safeguarding Officer and all trustees understand the issues and strategies at our school in relation to local and national guidelines and advice.

16.5. This policy, supported by the school's Acceptable Use Agreements for staff, trustees and governors, visitors, and students, is to protect the interests and safety of the whole school community. It is linked to the following mandatory school policies:

i. child protection.

ii. health and safety.

iii. home–school agreements.

iv. behaviour/student discipline (including the anti-bullying) policy and PSHE.

17. Online Safety in the Curriculum

17.1. ICT and online resources are increasingly used across the curriculum. We believe it is essential for online safety guidance to be given to the pupils on a regular and meaningful basis. Online safety is embedded within our curriculum, and we continually look for new opportunities to promote online safety.

17.2. The school has a framework for teaching internet skills in PSHE lessons which can be found in the PSHE schemes of work.

17.3. The school provides opportunities within a range of curriculum areas to teach about Online Safety.

17.4. Educating students about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-Safety curriculum.

17.5. Students are aware of the relevant legislation when using the internet such as data protection and intellectual property which may limit what they want to do but also serves to protect them.

17.6. Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modelling, and appropriate activities.

17.7. Students are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Students are also aware of where to seek advice or help if they experience problems when using the internet and related technologies, i.e., parent/carer, teacher/trusted staff member, or an organisation such as Cybermentors, Childline or CEOP report abuse button.

17.8. Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

18. Online Safety Skills Development for Staff

18.1. Details of the ongoing staff training programme can be found in the main office.

18.2. New staff receive information on the school's Acceptable Use Agreements as part of their induction.

18.3. All staff have been made aware of their individual responsibilities relating to the safeguarding of children within the context of onlineSafety and know what to do in the event of misuse of technology by any member of the school community (see onlineSafety Co-Ordinator).

18.4. All staff are encouraged to incorporate onlineSafety activities and awareness within their curriculum areas and ensure they are adequately informed with up-to-date areas of concern.

19. Managing the School Online Safety Messages

19.1. We endeavour to embed Online Safety messages across the curriculum whenever the internet and/or related technologies are used.

19.2. The Online Safety Policy will be introduced to the students at the start of each school year.

19.3. Online Safety posters will be prominently displayed.

19.4. The key Online Safety advice will be promoted widely through the school displays, newsletters, class activities and so on.

19.5. We will participate in Safer Internet Day every February.

20. Incident Reporting, Online Safety & Infringements

20.1. Incident Reporting:

i. Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the school's relevant responsible person or online safety Coordinator. Additionally, all security breaches, lost/stolen equipment, or data (including remote-access credentials and authentication information), virus notifications, unsolicited emails,

misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

20.2. Online Safety Incident Log:

i. Some incidents may need to be recorded if they relate to a bullying, prejudice based or discriminatory behaviour, extremism, or another safeguarding concern.

20.3. Complaints:

i. Complaints and/ or issues relating to online Safety should be made to the Online Safety Safeguarding Officer or Headteacher.

ii. All incidents should be logged.

20.4. Inappropriate Material:

i. All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the e-Safety Safeguarding Officer.

ii. Deliberate access to inappropriate materials by any user will lead to the incident being logged by the relevant responsible person, and an investigation by the Headteacher. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

21. Internet Access

21.1. The internet is an open worldwide communication medium, available to everyone. Anyone can view information, send messages, discuss ideas, and publish material which makes it both an invaluable resource for education, business, and social interaction, as well as a potential risk to young and vulnerable people.

21.2. Managing the Internet:

i. The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.

ii. Staff will preview any recommended sites, online services, software, and apps before use.

iii. Searching for images through open search engines is discouraged when working with students.

iv. If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

v. All users must always observe software copyright. It is illegal to copy or distribute school software or illegal software from other sources.

vi. All users must observe copyright of materials from electronic resources.

21.3. Internet Use:

i. You must not post personal, sensitive, confidential, or classified information or disseminate such information in any way that may compromise the intended restricted audience.

ii. Do not reveal names of colleagues, students, others, or any other confidential information acquired through your job on any social networking site or other online application.

iii. On-line gambling or gaming is not allowed.

iv. It is at the Head Teacher's discretion as to what internet activities are permissible for staff and students and how this is disseminated.

21.4. Infrastructure:

i. The Vine Christian School is aware of its responsibility when monitoring staff communication under current legislation and considers; Data Protection Act 2018, The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000, Human Rights Act 1998.

ii. Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.

iii. The school does not allow students access to internet logs.

iv. The school uses management control tools for controlling and monitoring workstations.

v. If staff or students discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the online safety coordinator or teacher as appropriate.

vi. It is the responsibility of the school, by delegation to the network manager, to ensure that security or endpoint-protection software is installed and kept up to date on all school machines.

vii. Students and Staff using personal removable media are responsible for measures to protect against viruses, for example making sure that additional systems used have up-to-date security or endpoint-protection software. It is neither the school's responsibility nor the network managers responsibility to install or maintain security or endpoint protection software on personal devices. If students wish to bring in work on removable media, it must be given to their supervisor for a safety check first.

viii. Students and staff are not permitted to download programs or files on school-based technologies without seeking prior permission from the Headteacher and ICT subject leader.

ix. If there are any issues related to malware, viruses or endpoint-protection software the network manager should be informed via email.

22. Managing Other Online Technologies

22.1. Online technologies (including social networking sites, if used responsibly both outside and within an educational context) can provide easy to use, creative, collaborative, and free facilities. However, it is important to recognise that there are issues regarding the appropriateness of some content, contact, culture, and commerce. To this end, we encourage our students to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

22.2. At present, the school endeavours to deny access to social networking and online games websites to students within school.

22.3. All students are advised to be cautious about the information given by others on such websites, for example users not being who they say they are.

22.4. Students are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

22.5. Students are always reminded to avoid giving out personal details on websites which may identify them or where they are (full name, address, mobile/home phone numbers, school details, IM/email address, specific hobbies/interests).

22.6. Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.

22.7. Students are encouraged to be wary about publishing specific and detailed private thoughts and information online.

22.8. Our students are asked to report any incidents of Cyberbullying to the school.

22.9. Staff may only create blogs, wikis, or other online areas to communicate with students using the school-approved learning platform or other systems approved by the Headteacher.

22.10. Online services may have minimum-age requirements. Pupils should comply with the minimum-age requirements of the individual services they use.

23. Parental Involvement

23.1. We believe that it is essential for parents/carers to be fully involved with promoting online Safety both in and outside of school and to be aware of their responsibilities. We regularly consult and discuss online Safety with parents/carers and seek to promote a wide understanding of the benefits of new technologies, together with the associated risks.

23.2. Parents/carers are asked to read through and sign Acceptable Use Agreements on behalf of their child on admission to the school.

23.3. Parents/carers are required to decide as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website).

23.4. Parents/carers are expected to sign an Acceptable Use Agreement.

23.5. The school disseminates information to parents relating to online safety where appropriate in the form of:

i. School website information

ii. Newsletter items

24. Passwords and Password Security

24.1. Passwords:

i. Always use your own personal passwords.

ii. Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

iii. Staff should change temporary passwords at first logon.

iv. Change passwords whenever there is any indication of possible system or password compromise.

v. Do not record passwords or encryption keys on paper or in an unprotected file.

vi. Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else. Ensure that all personal passwords that have been disclosed are changed once the requirement is finished.

vii. Never tell a child or colleague your password.

viii. If you aware of a breach of security with your password or account inform Mrs. René Esterhuizen immediately.

ix. Passwords must meet the school's current technical security requirements and DfE/NCSC guidance. Compromised or suspected compromised passwords must be changed immediately.

x. Multi-factor authentication will be enabled for staff accounts accessing cloud services or remotely accessing on-site systems, and for IT administrative accounts, where required by current DfE cyber-security standards.

xi. User ID and passwords for staff and students who have left the school are removed from the system within 30 days.

xii. If you think your password may have been compromised or someone else has become aware of your password report this to your Headteacher.

xiii. Do not use the same password for multiple accounts.

24.2. Password Security:

i. Password security is essential for staff, particularly as they can access and use student data. Staff are expected to have secure passwords which are not shared with anyone. The students are expected to keep their passwords private and not to share with others, particularly their friends. Staff and students are regularly reminded of the need for password security.

ii. All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.

iii. Users are provided with an individual network, email, learning platform and Management Information System log-in username.

iv. Students are not permitted to deliberately access on-line materials or files on the school network or local storage devices of their peers, teachers, or others.

v. Staff are aware of their individual responsibilities to protect the security and confidentiality of the school networks, MIS systems and/or learning platform, including ensuring that passwords are not shared and are changed immediately if compromised or suspected to be compromised. Individual staff users must also make sure that workstations are not left unattended and are locked.

vi. Due consideration should be given when logging into the school-approved learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

24.3. Dormant and Unused Accounts:

i. Accounts belonging to users who have left the school or who no longer require access must be disabled promptly to prevent unauthorised access.

25. Personal or Sensitive Information

25.1. Protecting Personal, Sensitive, Confidential and Classified Information:

i. Ensure that any school information accessed from your own device or removable media equipment is kept secure and remove any portable media from computers when not attended.

ii. Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

iii. Ensure the accuracy of any personal, sensitive, confidential, and classified information you disclose or share with others.

iv. Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person.

v. Ensure the security of any personal, sensitive, confidential, and classified information contained in documents you copy, scan or print. This is particularly important when shared Copiers (multi-function print, scan, and copiers) are used and when access is from a non-school environment.

vi. Only download personal data from systems if expressly authorised to do so by your manager.

vii. You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

viii. Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information.

ix. Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling.

25.2. Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media:

i. Ensure removable media is purchased with encryption.

ii. Store all removable media securely.

iii. Securely dispose of removable media that may hold personal data.

iv. Encrypt all files containing personal, sensitive, confidential, or classified data.

v. Ensure hard drives from machines no longer in service are removed and stored securely or wiped clean.

25.3. Guidance on How to Encrypt Files can be found on the ICO website:

https://ico.org.uk/media/for-organisations/encryption-1-0.pdf

26. Remote Access

26.1. Staff Responsibilities:

i. Staff are responsible for all activity carried out using their remote-access credentials.

ii. Remote access to school systems must use school-approved secure methods and devices and must be protected by appropriate authentication, including multi-factor authentication where required.

iii. Remote-access credentials, authentication codes and other security information must be kept confidential and must not be shared.

iv. Remote access should only be enabled for authorised users where it is required and should be disabled when no longer needed. Where appropriate, a secure virtual private network (VPN) or other approved encrypted connection should be used.

v. School information and data must remain protected when accessed remotely, particularly when using networks or devices outside the school.

27. Safe Use of Images

27.1. Taking of Images and Film:

i. The following applies to all parts of the school including the Early Years and Reception class.

ii. Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public, without first seeking consent and considering the appropriateness.

iii. With the written consent of parents (on behalf of students) and staff, the school permits the appropriate taking of images by staff and students with school equipment.

iv. Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of students, this includes when on field trips. However, with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

v. Students are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of students, staff, and others without advance permission from the Head Teacher.

vi. Students and staff must have permission from the Headteacher before any image can be uploaded for publication.

27.2. Consent of Adults Who Work at the School:

i. Permission to use images of all staff who work at the school is sought on induction and a copy is in the personnel file.

27.3. Publishing Student's Images and Work:

i. On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work/photos in the following ways:

ii. on the school web site.

iii. in the school prospectus and other printed publications that the school may produce for promotional purposes.

iv. recorded or transmitted on a video or webcam.

v. on the school-approved learning platform or online learning service.

vi. in display material that may be used in the school's communal areas.

vii. in display material that may be used in external areas, i.e., exhibition promoting the school.

viii. general media appearances, e.g., local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

ix. This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g., divorce of parents, custody issues, etc.

x. Parents or carers may withdraw permission, in writing, at any time. Consent must also be given in writing and will be kept on record by the school.

xi. Students' names will not be published alongside their image and vice versa. Email and postal addresses of students will not be published. Students' full names will not be published.

xii. Before posting student work on the Internet, a check needs to be made to ensure that permission has been given for work to be displayed.

xiii. Only Mr Dave Walker has authority to upload to the internet.

27.4. Storage of Images:

i. Images and films will only be taken, used, stored or shared where the school has an appropriate lawful basis under data protection law. Where the school relies on consent, written consent will be obtained and may be withdrawn in accordance with the school's Data Protection Policy and privacy information.

ii. Students and staff are not permitted to use personal portable media for storage of images (e.g., USB storage devices or other removable media) without the express permission of the Headteacher.

iii. Rights of access to this material are restricted to the teaching staff and students within the confines of the school network or other online school resource.

27.5. Webcams and CCTV:

i. The school uses CCTV for security and safety. Notification of CCTV use is displayed at the front of the school. For further guidance, please refer to this document: https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/

ii. We do not use publicly accessible webcams in school.

iii. Webcams will not be used for broadcast on the internet without prior parental consent.

iv. Misuse of the webcam by any member of the school community will result in sanctions (as listed under the 'inappropriate materials' section of this document).

27.6. Video Conferencing:

i. Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school.

ii. All students are supervised by a member of staff when video conferencing.

iii. The school keeps a record of video conferences, including date, time, and participants.

iv. Approval from the Head Teacher is sought prior to all video conferences within school to end-points beyond the school.

v. The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

vi. No part of any video conference is recorded in any medium without the written consent of those taking part.

27.7. Additional points to consider:

i. Participants in conferences offered by 3rd party organisations may not be DBS checked.

ii. Conference supervisors need to be familiar with how to use the video conferencing equipment, particularly how to end a call if at any point any person taking part becomes unhappy with the content of the conference.

28. School ICT Equipment

28.1. ICT Equipment:

i. As a user of the school ICT equipment, you are responsible for your activity.

ii. It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.

iii. Do not allow your visitors to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT facilities if available.

iv. Ensure that all ICT equipment that you use is kept physically secure.

v. Do not attempt unauthorised access or make unauthorised modifications to computer equipment, programs, files, or data. This is an offence under the Computer Misuse Act 1990.

vi. It is imperative that you save your data on a frequent basis to the school's network. You are responsible for the backup and restoration of any of your data that is not held on the school's network.

vii. Personal or sensitive data should not be stored on the local drives of desktop devices, laptops, USB storage devices or other removable media . If it is necessary to do so the local drive must be encrypted

viii. It is recommended that a time locking screensaver is applied to all machines. Any device accessing personal data must have a locking screensaver as must any user profiles.

ix. Privately owned ICT equipment should not be used on a school network.

x. On termination of employment, resignation, or transfer, return all school ICT equipment to the school. You must also provide details of all your system login credentials so that they can be disabled.

xi. It is your responsibility to ensure that any information accessed from your own device or removable media equipment is kept secure, and that no personal, sensitive, confidential, or classified information is disclosed to any unauthorised person.

xii. All ICT equipment allocated to staff must be authorised by the Head Teacher.

28.2. Portable & Mobile ICT Equipment:

i. This section covers such items as laptops, mobile devices, and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

ii. All activities carried out on school systems and hardware will be monitored in accordance with the general policy.

iii. Staff must ensure that all school data is stored on the school network and not kept solely on a single device. Any equipment where personal data is likely to be stored must be encrypted.

iv. Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

v. Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.

vi. Ensure portable and mobile ICT equipment is made available as necessary for security updates and software installations, patches, or upgrades.

vii. The installation of any applications or software packages must be authorised by the ICT support team, fully licensed and only carried out by your ICT support.

viii. In areas where there are likely to be members of the public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.

ix. Portable equipment must be transported in its protective case if supplied.

28.3. Mobile Technologies:

i. Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Mobile technologies such smartphones, tablets, and iPads, gaming devices, are generally very familiar to children outside of school. They often provide a collaborative, well-known device with possible internet access and thus open risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed. Our school chooses to manage the use of these devices in the following ways so that users exploit them appropriately.

28.4. Personal Mobile Devices (Including Mobile Phones):

i. The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a student or parent/ carer using their personal device.

ii. From 1 September 2026 the school will operate as a mobile-phone-free environment by default throughout the school day, in line with statutory DfE guidance. Any permitted exceptions, including reasonable adjustments or arrangements for medical, safeguarding or other individual needs, will be set out in the school's mobile-phone arrangements and applied consistently.

iii. This technology may be used for educational purposes, as mutually agreed with the Head Teacher. The device user, in this instance, must always ask the prior permission of the bill payer.

iv. The school is not responsible for the loss, damage, or theft of any personal mobile device.

v. The sending of inappropriate text messages between any member of the school community is not allowed.

vi. Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.

vii. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.

viii. Never use a hand-held mobile phone whilst driving a vehicle.

28.5. School Provided Mobile Devices (Including Phones):

i. The school does not provide any mobile devices.

28.6. Telephone Services:

i. You may make or receive personal telephone calls provided:

- They are infrequent, kept as brief as possible and do not cause annoyance to others.
- They are not for profit or to premium rate services.
- They conform to this and other relevant school policies.

ii. School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.

iii. Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

iv. Ensure that your incoming telephone calls can always be handled.

v. Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available in the main office. If you do not have a copy, please ask the Headteacher.

28.7. Removable Media:

i. If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section'. Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

ii. Ensure the accuracy of any personal, sensitive, confidential, and classified information you disclose or share with others.

iii. Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person.

iv. Ensure the security of any personal, sensitive, confidential, and classified information contained in documents you copy, scan, or print. This is particularly important when shared Copiers (multi-function print, scan, and copiers) are used and when access is from a non-school environment.

v. Only download personal data from systems if expressly authorised to do so by your manager.

vi. You must not post on the internet personal, sensitive, confidential, or classified information, or disseminate such information in any way that may compromise its intended restricted audience.

vii. Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information.

viii. Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labelling

28.8. Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media

i. Always consider if an alternative solution already exists.

ii. Only use recommended removable media.

iii. Encrypt and password protect.

iv. Store all removable media securely.

v. Removable media must be disposed of securely by your ICT support team.

29. Social media

29.1. School communication platforms:

i. Social media platforms and services are an established part of online communication. Our school uses, Microsoft Teams and WhatsApp to communicate with parents and carers. Mrs. René Esterhuizen is responsible for all postings on these technologies and monitors responses from others.

29.2. Social media code of conduct:

i. Staff are not permitted to access their personal social media accounts using school equipment at any time during school hours.

ii. Staff can setup school-approved online learning platforms, using their school email address, to be able to teach students the safe and responsible use of Social Media.

iii. Students are not permitted to access their social media accounts whilst at school.

iv. Students must not access personal social-media accounts during the school day except where an expressly authorised exception applies under the school's mobile-phone and online-safety arrangements.

v. Staff, Trustees and Governors, students, parents, and carers are regularly provided with information on how to use social media responsibly and what to do if they are aware of inappropriate use by others.

vi. Staff, Trustees and Governors, students, parents, and carers are aware that the information, comments, images, and video they post online can be viewed by others, copied, and stay online forever.

vii. Staff, Trustees and Governors, students, parents, and carers are aware that their online behaviour should always be compatible with UK law.

30. Servers

30.1. The Vine Christian School abides by the following criteria:

i. Always keep servers in a locked and secure environment.

ii. Limit access rights.

iii. Always password protect and lock the server.

iv. Existing servers should have security software installed appropriate to the machine's specification.

v. Data must be backed up regularly.

vi. Backups must be encrypted where appropriate and stored securely, with appropriate off-site or logically separate backup arrangements

31. Systems and Access

31.1. Staff Responsibilities:

i. You are responsible for all activity on school systems carried out under any access/account rights assigned to you, whether accessed via school ICT equipment or your own device.

ii. Do not allow any unauthorised person to use school ICT facilities and services that have been provided to you.

iii. Ensure you remove portable media from your computer when it is left unattended.

iv. Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.

v. Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information.

vi. Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential, or otherwise classified data and to prevent unauthorised access.

vii. Ensure that you logoff from the computer completely when you are going to be away from the it for a longer period.

viii. Do not introduce or propagate viruses.

ix. Staff must not use school systems to access, create, load, store, post or send illegal, harmful, discriminatory, pornographic, defamatory or otherwise inappropriate material. This includes content which may breach safeguarding requirements or the Equality Act 2010. Any suspected illegal or safeguarding content must be reported promptly in accordance with this policy and the Safeguarding and Child Protection Policy.

x. Where necessary, permission must be obtained from the rights holder before using, copying or distributing material protected by the Copyright, Designs and Patents Act 1988.

xi. It is essential that any hard drives which may have held personal or confidential data are 'scrubbed' in a way that means the data can no longer be read. It is not sufficient to simply delete the files or reformat the hard drive. Whoever is appointed to dispose of the equipment must provide written confirmation that the data will be irretrievably destroyed using an appropriate secure data-erasure method.