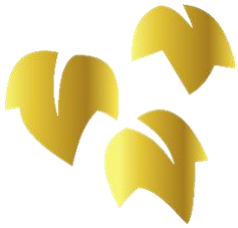

THE VINE CHRISTIAN SCHOOL

Independent School - Ages 3 to 18

Online E-Safety Policy

VCS/Online E-Safety Policy/2021

24 March 2021

The Vine Christian School, Basingstoke Road, Reading, RG7 1AT
Charity Number: 1104385 Tel: +44 (0) 118 988 6464 Email: office@thevcs.org.uk

About This Document

Annual Policy Period	2020 - 2021
Policy Adopted by Governors	September 2019
Last Policy Review	24 March 2021
Next Policy Review	September 2021

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.

Contents

1. Introduction 4
2. Data protection 5
3. Monitoring....5
4. Breaches 5
5. Incident reporting 6
6. Computer viruses 6
7. Data security 6
8. Security....7
9. Protective marking of official information 7
10. Relevant responsible persons 8
11. Information asset owner (iao) 8
12. Disposal of redundant ict equipment policy 8
13. Email 10
14. Equal opportunities: students with additional needs 12
15. E-safety roles and responsibilities....12
16. E-safety in the curriculum 13
17. E-safety skills development for staff 13
18. Managing the school e-safety messages 13
19. Incident reporting, e-safety & infringements 14
20. Internet access 14
21. Managing other online technologies 16
22. Parental involvement 16
23. Passwords and password security 17
24. Personal or sensitive information 18
25. Remote access....19
26. Safe use of images....19
27. School ict equipment 21
28. Social media 24
29. Servers....24
30. Systems and access 25
31. Key dates for the plan 26
32. General 26

1. Introduction

1.1. This policy should be read in conjunction with the following policies and guidance:

i. Safeguarding and Child Protection

ii. Data Protection

iii. Keeping Children Safe in Education 2020

1.2. At The Vine Christian School, we understand the responsibility to educate our students on online safety issues (e-safety); 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. 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.

1.5. 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, including Facebook and Twitter.

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

vi. Other mobile devices including tablets and gaming devices.

vii. Online Games.

viii. Learning Platforms and Virtual Learning Environments.

ix. Blogs and Wikis.

x. Podcasting.

xi. Video sharing.

xii. Downloading.

xiii. On demand TV and video, movies, and radio / Smart TVs.

1.6. 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 some have minimum age requirements (13 years in most cases).

1.7. 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.

1.8. 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.

1.9. 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 PCs, laptops, mobile devices, webcams, whiteboards, voting systems, 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 GDPR.

3. Monitoring

3.1. All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the Data Protection Act 2018, the Human Rights Act 1998, the Regulation of Investigatory Powers Act 2000 (RIPA) and the Lawful Business Practice Regulations 2000.

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

4. Breaches

4.1. 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.

4.2. 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.

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

4.4. The Information Commissioner's powers to issue monetary penalties came into force on 6 April 2010, allowing the Information Commissioner's office to serve notices requiring organisations to pay up to £500,000 for serious breaches of the Data Protection Act.

4.5. The data protection powers of the Information Commissioner's Office are to:

i. Conduct assessments to check organisations are complying with the Act.

ii. Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time.

iii. Serve enforcement notices and 'stop now' orders where there has been a breach of the Act, requiring organisations to take (or refrain from taking) specified steps to ensure they comply with the law.

iv. Prosecute those who commit criminal offences under the Act.

v. Conduct audits to assess whether organisations' processing of personal data follows good practice.

vi. Report to Parliament on data protection issues of concern.

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

5. Incident Reporting

5.1. 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 ID and PINs), 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, Mr. Babu Samuel and Mrs. Naomi Spooner.

5.2. Please refer to the relevant section on Incident Reporting, e-Safety Incident Log & Infringements.

6. Computer Viruses

6.1. All files downloaded from the Internet, received via email or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.

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

6.3. If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.

6.4. If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact your ICT support provider immediately. The ICT support provider will advise you what actions to take and be responsible for advising others that need to know.

7. Data Security

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

7.2. Security of Confidential / 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. Storage devices such USB sticks 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.

8. Security

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

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

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

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

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

8.6. 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.

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

8.8. 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.

9. Protective Marking of Official Information

9.1. Staff must be trained to understand that they are personally responsible for securely handling any information that is entrusted to them, in line with local business processes.

9.2. There is no requirement to mark routine OFFICIAL information.

9.3. Optional descriptors can be used to distinguish specific type of information.

9.4. Use of descriptors is at an organisation's discretion.

9.5. Existing information does not need to be remarked.

9.6. In such cases where there is a clear and justifiable requirement to reinforce the 'need to know', assets should be conspicuously marked: 'OFFICIAL–SENSITIVE.'

10. Relevant Responsible Persons

10.1. Senior members of staff should be familiar with information risks and the school's response. Sometimes called a SIRO, there should be a member of the senior leadership team who has the following responsibilities:

i. they lead on the information risk policy and risk assessment.

ii. they advise school staff on appropriate use of school technology.

iii. they act as an advocate for information risk management.

10.2. The Office of Public Sector Information has produced Managing Information Risk, [http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf] to support relevant responsible staff members in their role.

10.3. The SIRO in this school is Mr. Babu Samuel

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. As a result, this manager 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. All redundant ICT equipment that may have held personal data will have the storage media over written multiple times 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 2006

ii. The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

- http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx
- http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf
- http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

iii. Data Protection Act 2018

- https://ico.org.uk/for-organisations/education/

iv. Electricity at Work Regulations 1989

- http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

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 be held the storage media will be over written multiple times 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. Environment Agency web site

iii. Introduction

- http://www.environment-agency.gov.uk/business/topics/waste/32084.aspx

iv. The Waste Electrical and Electronic Equipment Regulations 2006

- http://www.opsi.gov.uk/si/si2006/uksi_20063289_en.pdf

v. The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

- http://www.opsi.gov.uk/si/si2007/pdf/uksi_20073454_en.pdf?lang=_e

vi. Information Commissioner Website

- https://ico.org.uk/

vii. Data Protection Act – data protection guide

- https://ico.org.uk/for-organisations/education/

13. Email

13.1. 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.

13.2. 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 your school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. You must therefore actively manage your email account 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 e-Safety coordinator or Headteacher) if they receive an offensive email.

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.

13.3. 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.

13.4. 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.

13.5. 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.

14. Equal Opportunities: Students with Additional Needs

14.1. The school endeavours to create a consistent message with parents for all students and this in turn should aid establishment and future development of the schools' e-Safety rules.

14.2. However, staff should be aware that some students may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-Safety issues.

14.3. Where a student has poor social understanding, careful consideration should be given to group interactions when raising awareness of e-Safety. Internet activities should be planned and well managed for these children and young people.

15. E-safety Roles and Responsibilities

15.1. As e-Safety is an important aspect of strategic leadership within the school, the headteacher, trustees and governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

15.2. The named e-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.

15.3. It is the role of the e-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.

15.4. Trustees and Governors are updated by the e-Safety Safeguarding Officer. All trustees and governors understand the issues and strategies at our school in relation to local and national guidelines and advice.

15.5. 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.

16. E-safety in the Curriculum

16.1. ICT and online resources are increasingly used across the curriculum. We believe it is essential for e-Safety guidance to be given to the students on a regular and meaningful basis. E-Safety is embedded within our curriculum and we continually look for new opportunities to promote e-Safety.

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

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

16.4. 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.

16.5. 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.

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

16.7. 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.

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

17. E-safety Skills Development for Staff

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

17.2. New staff receive information on the school's acceptable use policy as part of their induction.

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

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

18. Managing the School e-Safety Messages

18.1. We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.

18.2. The e-Safety policy will be introduced to the students at the start of each school year.

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

19. Incident Reporting, e-Safety & Infringements

19.1. 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 e-Safety Co-Ordinator. Additionally, all security breaches, lost/stolen equipment or data (including remote access ID and PINs), virus notifications, unsolicited emails, misuse or unauthorised use of ICT and all other policy non-compliance must be reported to the Information Asset Owner.

19.2. E-Safety Incident Log:

i. Some incidents may need to be recorded if they relate to a bullying, extremism, or racist incident.

19.3. Complaints:

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

ii. All incidents should be logged.

19.4. 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.

20. Internet Access

20.1. 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.

20.2. 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.

20.3. 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.

20.4. Infrastructure:

i. Our school employs some additional web-filtering.

ii. IT use is monitored using a proactive monitoring system.

iii. However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.

iv. 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.

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

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

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

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

ix. It is the responsibility of the school, by delegation to the network manager, to ensure that anti-virus protection is installed and kept up to date on all school machines.

x. 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 virus protection software. It is neither the school's responsibility nor the network managers to install or maintain virus protection on personal systems. If students wish to bring in work on removable media, it must be given to their Supervisor for a safety check first.

xi. 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.

xii. If there are any issues related to viruses or anti-virus software, the network manager should be informed via email.

21. Managing Other Online Technologies

21.1. 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 commercialism. 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.

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

21.3. 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.

21.4. 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.

21.5. 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).

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

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

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

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

22. Parental Involvement

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

22.2. Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.

22.3. 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).

22.4. Parents/carers are expected to sign an acceptable use agreement.

22.5. The school disseminates information to parents relating to e-Safety where appropriate in the form of:

i. School website information

ii. Newsletter items

23. Passwords and Password Security

23.1. 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 contain a minimum of six characters and be difficult to guess.

x. Passwords should contain a mixture of upper and lowercase letters, numbers, and symbols.

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 Head Teacher.

23.2. 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 periodically. 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 learning platform, virtual learning environment or other online application to the browser/cache options (shared or private computer)

23.3. Zombie Accounts:

i. 'Zombie accounts' refers to accounts belonging to users who have left the school and therefore no longer have authorised access to the school's systems. Such Zombie accounts when left active can cause a security threat by allowing unauthorised access.

ii. Ensure that all user accounts are disabled once the member of the school has left.

iii. Prompt action on disabling accounts will prevent unauthorized access.

iv. Regularly change generic passwords to avoid unauthorised access.

24. Personal or Sensitive Information

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

i. Ensure that any school information accessed from your own PC 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.

24.2. 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.

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

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

25. Remote Access

25.1. Staff Responsibilities:

i. You are responsible for all activity via your remote access facility.

ii. Only use equipment with an appropriate level of security for remote access

iii. To prevent unauthorised access to school systems, keep all dial-up access information such as telephone numbers, logon IDs and PINs confidential and do not disclose them to anyone.

iv. Select PINs to ensure that they are not easily guessed, e.g., do not use your house, or telephone number or choose consecutive or repeated numbers.

v. Avoid writing down or otherwise recording any network access information. Any such information that is written down must be kept in a secure place and disguised so that no other person will be able to identify what it is.

vi. Always protect school information and data, including any printed material produced while using the remote access facility. Take particular care when access is from a non-school environment.

26. Safe Use of Images

26.1. 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.

26.2. 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.

26.3. 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/ transmitted on a video or webcam.

v. on the school's learning platform or Virtual Learning Environment.

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 the ICT Manager, Mrs. Marilynn Williams or Mrs. Naomi Spooner has authority to upload to the internet.

26.4. Storage of Images:

i. In line with GDPR images are used only with the written consent of parents/carers which is secured in the first instance on a child's entry to the school. Records are kept on file and consent can be changed by parents/carers at any time.

ii. Students and staff are not permitted to use personal portable media for storage of images (e.g., USB sticks) without the express permission of the Head Teacher.

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.

26.5. 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).

26.6. 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.

26.7. Additional points to consider:

i. Participants in conferences offered by 3rd party organisations may not be DBS (previously CRB) 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.

27. School ICT Equipment

27.1. 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 PC, laptop, USB memory stick or another portable device. 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 logons so that they can be disabled.

xi. It is your responsibility to ensure that any information accessed from your own PC 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.

27.2. 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 the laptop. 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 anti-virus 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.

27.3. 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, Blackberries, iPads, games players, 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.

27.4. Personal Mobile Devices (Including 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. Students can bring personal mobile devices/phones to school but must not use them for personal purposes within lesson time. At all times, the device must be switched onto silent.

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.

27.5. School Provided Mobile Devices (Including Phones):

i. The school does not provide any mobile devices.

27.6. 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 HCC and 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.

27.7. Removable Media:SS

i. If storing or transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section '

ii. Always consider if an alternative solution already exists.

iii. Only use recommended removable media.

iv. Encrypt and password protect.

v. Store all removable media securely.

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

28. Social media

28.1. School communication platforms:

i. Facebook, Twitter, and other forms of social media are increasingly becoming an important part of our daily lives. Our school uses Seesaw, 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.

28.2. 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 Social Learning Platform accounts, 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. 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.

v. 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.

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

29. Servers

29.1. 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. Backup tapes should be encrypted by appropriate software.

vi. Data must be backed up regularly.

vii. Backup tapes/discs must be securely stored in a fireproof container.

viii. Back up media stored off-site must be secure.

30. Systems and Access

30.1. 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 PC.

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 PC completely when you are going to be away from the computer for a longer period.

viii. Do not introduce or propagate viruses.

ix. It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be, illegal, offensive, libellous, pornographic, obscene, defamatory, intimidating, misleading or disruptive to the school or may bring the school or HCC into disrepute. This includes, but is not limited to, jokes, chain letters, files, emails, clips, or images that are not part of the school's business activities; sexual comments or images, nudity, racial slurs, gender specific comments, or anything that would offend someone on the basis of their age, sexual orientation, religious or political beliefs, national origin, or disability (in accordance with the Sex Discrimination Act, the Race Relations Act and the Disability Discrimination Act).

x. Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.

xi. Where necessary, obtain permission from the owner or owning authority and pay any relevant fees before using, copying, or distributing any material that is protected under the Copyright, Designs and Patents Act 1998.

xii. 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 you appoint to dispose of the equipment must provide a written guarantee that they will irretrievably destroy the data by multiple over writing the data.

31. Key dates for the plan

Priority	Date	Action
Online E-Safety training	Annually	Prepare training for Autumn term.
Online E-Safety audit	Bi-annually	Update current audit to reflect actions that have been completed.

32. General

Signed by school personnel as follows:

Head teacher	Signed	Date	Print name
Governor	Signed	Date	Print name