THE VINE CHRISTIAN SCHOOL
Independent School - Ages 3 to 18

ONLINE & E-SAFETY POLICY

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

- Safeguarding and Child Protection
- Data Protection
- Keeping Children Safe in Education 2020

INTRODUCTION

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.

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.

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.

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:

- Websites
- Apps
- E-mail, Instant Messaging, and chat rooms
- Social Media, including Facebook and Twitter
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices including tablets and gaming devices
- Online Games
- Learning Platforms and Virtual Learning Environments
- Blogs and Wikis
- Podcasting
- Video sharing
- Downloading
- On demand TV and video, movies, and radio / Smart TVs

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).

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.

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.

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).

DATA PROTECTION

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

MONITORING

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

BREACHES

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.

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.

Policy breaches may also lead to criminal or civil proceedings.

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.

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

- Conduct assessments to check organisations are complying with the Act.
- Serve information notices requiring organisations to provide the Information Commissioner's Office with specified information within a certain time.
- 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.
- Prosecute those who commit criminal offences under the Act.
- Conduct audits to assess whether organisations' processing of personal data follows good practice,
- Report to Parliament on data protection issues of concern

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

INCIDENT REPORTING

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 Mr. Michael Spooner.

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

COMPUTER VIRUSES

- All files downloaded from the Internet, received via e-mail or on removable media such as a memory stick must be checked for any viruses using school provided anti-virus software before being used.
- Never interfere with any anti-virus software installed on school ICT equipment.
- If your machine is not routinely connected to the school network, you must make provision for regular virus updates through your IT team.
- 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.

DATA SECURITY

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

Security of Confidential / Personal Data - Electronic and Paper

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

- We will ensure that **ALL** staff are aware of how to handle sensitive or personal information.
- Storage devices such USB sticks are best encrypted in their entirety.
- Staff laptops that hold personal data should have an encrypted 'container' created where all sensitive data should be stored.
- Backup media must always be kept secure.

SECURITY

- The school gives relevant staff access to its Management Information System, with a unique username and password.
- It is the responsibility of everyone to keep passwords secure.
- Staff are aware of their responsibility when accessing school data.
- Staff have been issued with the relevant guidance documents and the Policy for ICT Acceptable Use.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential, or classified data.
- 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.
- Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and always keep it under your control.
- 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.

PROTECTIVE MARKING OF OFFICIAL INFORMATION

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.

- There is no requirement to mark routine OFFICIAL information.
- Optional descriptors can be used to distinguish specific type of information.
- Use of descriptors is at an organisation's discretion.
- Existing information does not need to be remarked.

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

RELEVANT RESPONSIBLE PERSONS

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:

- they lead on the information risk policy and risk assessment
- they advise school staff on appropriate use of school technology
- they act as an advocate for information risk management

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.

The SIRO in this school is Mr. Babu Samuel

INFORMATION ASSET OWNER (IAO)

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

- what information is held, and for what purposes.
- what information needs to be protected, how information will be amended or added to over time.
- who has access to the data and why?
- how information is retained and disposed of.

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.

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.

The IAO in this school is Mrs. René Esterhuizen

DISPOSAL OF REDUNDANT ICT EQUIPMENT POLICY

- 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

- 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.

- Disposal of any ICT equipment will conform to:

  The Waste Electrical and Electronic Equipment Regulations 2006
  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

  Data Protection Act 2018

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

  Electricity at Work Regulations 1989

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

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

- The school's disposal record will include:

  - ✓ Date item disposed of
  - ✓ Authorisation for disposal, including:
  - ✓ verification of software licensing
  - ✓ any personal data* likely to be held on the storage media?
  - ✓ How it was disposed of e.g. waste, gift, sale
  - ✓ Name of person & / or organisation who received the disposed item

*if personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed.

- 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

Further information available at:

Waste Electrical and Electronic Equipment (WEEE) Regulations

Environment Agency web site

Introduction

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

The Waste Electrical and Electronic Equipment Regulations 2006

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

The Waste Electrical and Electronic Equipment (Amendment) Regulations 2007

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

Information Commissioner Website

https://ico.org.uk/

Data Protection Act – data protection guide

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

EMAIL

The use of e-mail within most schools is an essential means of communication for both staff and students. In the context of school, e-mail should not be considered private. Educationally, e-mail 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 e-mail in relation to their age and how to behave responsible online.

Managing E-Mail

- The school gives all staff, Trustees and Governors their own e-mail 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 e-mails and avoids the risk of personal profile information being revealed.
- Staff, Trustees and Governors should use their school email for all professional communication.
- 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, e-mail histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact students, parents or conduct any school business using personal e-mail addresses.
- The school requires a standard disclaimer to be attached to all e-mail correspondence, stating that, 'the views expressed are not necessarily those of the school'. The responsibility for adding this disclaimer lies with the account holder.
- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending e-mails to external organisations, parents or students are advised to cc. the Headteacher.
- Students may only use school approved accounts on the school system and only under direct teacher supervision for educational purposes.
- E-mails 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 e-mail account as follows:

    - ✓ Delete all e-mails of short-term value
    - ✓ Organise e-mail into folders and carry out frequent housekeeping on all folders and archives.

- All student e-mail 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 e-mail communication, or arrange to meet anyone without specific permission, virus checking attachments.
- Students must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail.
- Staff must inform (the e-Safety coordinator or Head Teacher) if they receive an offensive e-mail.
- Students are introduced to e-mail as part of the Computing Programme of Study.
- In whatever way you access your school e-mail (whether directly, through webmail when away from the office or on non-school hardware) all the school e-mail policies apply.

Sending E-Mail

- If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section:
  E-Mailing Personal, Sensitive, Confidential or Classified Information
- Use your own school e-mail account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.
- Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.
- School e-mail is not to be used for personal advertising.

Receiving E-Mail

- Check your e-mail regularly.
- Activate your 'out-of-office' notification when away for extended periods.
- Never open attachments from an untrusted source.
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder.
- The automatic forwarding and deletion of e-mails is not allowed.

E-Mailing Personal, Sensitive, Confidential or Classified Information

Where your conclusion is that e-mail must be used to transmit such data obtain express consent from your Head Teacher to provide the information by e-mail and exercise caution when sending the e-mail and always follow these checks before releasing the e-mail:

- Encrypt and password protect.
- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
- Do not copy or forward the e-mail 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 e-mail.
- 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 e-mail.
- Request confirmation of safe receipt.

EQUAL OPPORTUNITIES: STUDENTS WITH ADDITIONAL NEEDS

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.

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.

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.

E-SAFETY ROLES AND RESPONSIBILITIES

As e-Safety is an important aspect of strategic leadership within the school, the Head Teacher, Trustees and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

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.

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.

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

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: child protection, health and safety, home–school agreements, and behaviour/student discipline (including the anti-bullying) policy and PSHE.

E-SAFETY IN THE CURRICULUM

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.

- The school has a framework for teaching internet skills in PSHE lessons which can be found in the PSHE schemes of work.
- The school provides opportunities within a range of curriculum areas to teach about Online Safety.
- 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.
- 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.
- Students are taught about copyright, respecting other people's information, safe use of images and other important areas through discussion, modeling, and appropriate activities.
- 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
- Students are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models, discussions and via the Computing curriculum.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- Details of the ongoing staff training programme can be found in the main office.
- New staff receive information on the school's acceptable use policy as part of their induction
- 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)
- 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.

MANAGING THE SCHOOL E-SAFETY MESSAGES

- We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-Safety policy will be introduced to the students at the start of each school year.
- We will participate in Safer Internet Day every February.

INCIDENT REPORTING, E-SAFETY & INFRINGEMENTS

Incident Reporting

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.

E-Safety Incident Log

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

MISUSE AND INFRINGEMENTS

Complaints

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

All incidents should be logged.

Inappropriate Material

- 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.
- 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.

INTERNET ACCESS

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.

Managing the Internet

- The school provides students with supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet connectivity.
- Staff will preview any recommended sites, online services, software, and apps before use.
- Searching for images through open search engines is discouraged when working with students.
- 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.
- All users must always observe software copyright. It is illegal to copy or distribute school software or illegal software from other sources.
- All users must observe copyright of materials from electronic resources

Internet Use

- You must not post personal, sensitive, confidential, or classified information or disseminate such information in any way that may compromise the intended restricted audience.
- 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.
- On-line gambling or gaming is not allowed.

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

Infrastructure

- Our school employs some additional web-filtering which is the responsibility of Martin Fuller who is the school's Network Manager.
- IT use is monitored using a pro-active monitoring system.
- However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.
- 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.
- Staff and students are aware that school-based email and internet activity can be monitored and explored further if required.
- The school does not allow students access to internet logs.
- The school uses management control tools for controlling and monitoring workstations.
- 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.
- 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.
- 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.
- 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.
- If there are any issues related to viruses or anti-virus software, the network manager should be informed via email.

MANAGING OTHER ONLINE TECHNOLOGIES

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.

- At present, the school endeavors to deny access to social networking and online games websites to students within school.
- 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.
- 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.
- 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).
- Our students are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals.
- Students are encouraged to be wary about publishing specific and detailed private thoughts and

information online.
- Our students are asked to report any incidents of Cyberbullying to the school.
- 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.
- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

PARENTAL INVOLVEMENT

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.

- Parents/carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to the school.
- 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).
- Parents/carers are expected to sign an acceptable use agreement.
- The school disseminates information to parents relating to e-Safety where appropriate in the form of:

✓ School website information
✓ Newsletter items

PASSWORDS AND PASSWORD SECURITY

Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.
- Staff should change temporary passwords at first logon.
- Change passwords whenever there is any indication of possible system or password compromise.
- Do not record passwords or encryption keys on paper or in an unprotected file.
- **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.
- **Never tell a child or colleague your password.**
- **If you aware of a breach of security with your password or account inform Mrs. René Esterhuizen immediately.**

- Passwords must contain a minimum of six characters and be difficult to guess.
- Passwords should contain a mixture of upper and lowercase letters, numbers, and symbols
- User ID and passwords for staff and students who have left the school are removed from the system within 30 days.

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

Password Security

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.

- All users read and sign an Acceptable Use Agreement to demonstrate that they have understood the school's e-Safety Policy and Data Security.
- Users are provided with an individual network, email, learning platform and Management Information System log-in username.
- 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.
- 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.
- 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)

Zombie Accounts

'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.

- Ensure that all user accounts are disabled once the member of the school has left.
- Prompt action on disabling accounts will prevent unauthorized access.
- Regularly change generic passwords to avoid unauthorised access.

PERSONAL OR SENSITIVE INFORMATION

Protecting Personal, Sensitive, Confidential and Classified Information

- 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.
- Ensure you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.
- Ensure the accuracy of any personal, sensitive, confidential, and classified information you disclose or share with others.
- Ensure that personal, sensitive, confidential, or classified information is not disclosed to any unauthorised person.
- 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.
- Only download personal data from systems if expressly authorised to do so by your manager
- 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.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information.
- Ensure hard copies of data are securely stored and disposed of after use in accordance with the document labeling.

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

- Ensure removable media is purchased with encryption.
- Store all removable media securely.
- Securely dispose of removable media that may hold personal data.
- Encrypt all files containing personal, sensitive, confidential, or classified data.

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

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

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

REMOTE ACCESS

- You are responsible for all activity via your remote access facility
- Only use equipment with an appropriate level of security for remote access
- 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
- 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
- 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
- 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

SAFE USE OF IMAGES

Taking of Images and Film

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

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.

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

Consent of Adults Who Work at the School

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

Publishing Student's Images and Work

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:

- on the school web site.
- in the school prospectus and other printed publications that the school may produce for promotional purposes.
- recorded/ transmitted on a video or webcam.
- on the school's learning platform or Virtual Learning Environment.

- in display material that may be used in the school's communal areas.
- in display material that may be used in external areas, i.e. exhibition promoting the school.
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically).

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.

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.

Students' names will not be published alongside their image and vice versa. E-mail and postal addresses of students will not be published. Students' full names will not be published.

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.

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

Storage of Images

- 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.
- 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.
- 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.

Webcams and CCTV

- The school uses CCTV for security and safety. The only people with access to this are **Mr. Deon Esterhuizen and Mr. Martin Fuller.** Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance https://ico.org.uk/about-the-ico/consultations/cctv-code-of-practice-revised/
- We do not use publicly accessible webcams in school.
- Webcams will not be used for broadcast on the internet without prior parental consent.
- 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).

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with endpoints outside of the school.
- All students are supervised by a member of staff when video conferencing.
- The school keeps a record of video conferences, including date, time, and participants
- Approval from the Head Teacher is sought prior to all video conferences within school to end-points beyond the school.
- The school conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.
- No part of any video conference is recorded in any medium without the written consent of those taking part.

Additional points to consider:

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

SCHOOL ICT EQUIPMENT INCLUDING PORTABLE & MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

School ICT Equipment

- As a user of the school ICT equipment, you are responsible for your activity.
- It is recommended that schools log ICT equipment issued to staff and record serial numbers as part of the school's inventory.
- 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.
- Ensure that all ICT equipment that you use is kept physically secure.
- 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.
- 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.
- 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
- 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.
- Privately owned ICT equipment should not be used on a school network.
- 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.
- 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.
- All ICT equipment allocated to staff must be authorised by the Head Teacher.

✓ maintaining control of the allocation.
✓ recovering and returning equipment when no longer needed.

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA).

Portable & Mobile ICT Equipment

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.

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

- Synchronise all locally stored data, including diary entries, with the central school network server on a frequent basis.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches, or upgrades.
- 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.
- 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.
- Portable equipment must be transported in its protective case if supplied.

MOBILE TECHNOLOGIES

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.

Personal Mobile Devices (Including Phones)

- 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.
- 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.
- 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.
- The school is not responsible for the loss, damage, or theft of any personal mobile device.
- The sending of inappropriate text messages between any member of the school community is not allowed.
- Permission must be sought before any image or sound recordings are made on these devices of any member of the school community.
- Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device.
- Never use a hand-held mobile phone whilst driving a vehicle.

School Provided Mobile Devices (Including Phones)

- The school does not provide any mobile devices.

Telephone Services

- You may make or receive personal telephone calls provided:

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

- School telephones are provided specifically for school business purposes and personal usage is a privilege that will be withdrawn if abused.
- 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.
- Ensure that your incoming telephone calls can always be handled.

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat. These procedures should be made readily available throughout your office. If you do not have a copy, please ask Mrs. René Esterhuizen.

Removable Media

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

- Always consider if an alternative solution already exists.
- Only use recommended removable media.
- Encrypt and password protect.
- Store all removable media securely.

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

SOCIAL MEDIA

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.
- Staff **are not** permitted to access their personal social media accounts using school equipment at any **time during school hours.**
- 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.
- Students are not permitted to access their social media accounts whilst at school.
- 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.
- 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.
- Staff, Trustees and Governors, students, parents and carers are aware that their online behaviour should always be compatible with UK law.

SERVERS

The Vine Christian School abides by the following criteria:

- Always keep servers in a locked and secure environment.
- Limit access rights.
- Always password protect and lock the server.
- Existing servers should have security software installed appropriate to the machine’s specification.
- Backup tapes should be encrypted by appropriate software.
- Data must be backed up regularly.
- Backup tapes/discs must be securely stored in a fireproof container.
- Back up media stored off-site must be secure.

SYSTEMS AND ACCESS

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

provided to you.

- Ensure you remove portable media from your computer when it is left unattended.
- Use only your own personal logons, account IDs and passwords and do not allow them to be used by anyone else.
- Keep your screen display out of direct view of any third parties when you are accessing personal, sensitive, confidential, or classified information.
- 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.
- Ensure that you logoff from the PC completely when you are going to be away from the computer for a longer period.
- Do not introduce or propagate viruses.
- It is imperative that you do not access, load, store, post or send from school ICT any material that is, or may be considered to be, illegal, offensive, libelous, 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).
- Any information held on School systems, hardware or used in relation to School business may be subject to The Freedom of Information Act.
- 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.

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.

REVIEWING THIS POLICY

Review Procedure

There will be on-going opportunities for staff to discuss with the e-Safety coordinator any e-Safety issue that concerns them.

There will be on-going opportunities for staff to discuss with the AIO any issue of data security that concerns them.

This policy will be reviewed every (24) months and consideration will be given to the implications for future whole school development planning.

The policy will be amended if new technologies are adopted or Central Government change the orders or guidance in any way.

This policy has been read, amended, and approved by the staff, head teacher, Trustees and Governors.

ACCEPTABLE USE AGREEMENTS

Student Acceptable Use Agreement / E-Safety Rules – Each student should receive a copy to read.

Primary Student Acceptable Use Agreement / e-Safety Rules – All parents/carers should read these with primary age children and sign to say they agree.

Senior Student Acceptable Use Agreement / e-Safety Rules – Students at this age can sign these for themselves.

Parent/Carer Acceptable Use Agreement / Code of Conduct – All parents/carers should read and sign this document.

Staff, Volunteer, Trustee, Governor and Visitor Acceptable Use Agreement / E-Safety / Code of Conduct – All staff, whether volunteers, trustees or governors, and visitors should read and sign this document.

Student Acceptable Use and E-Safety Rules

You should:

- **Only access the internet under the direct supervision of a member of staff, and never access the internet when a member of staff is not present in the same room.**
- Only access sites which are appropriate for use in school. Personal websites (e.g. Facebook, Instagram, Tumblr, Gmail) are **not** appropriate for use in school
- Be aware that your actions on the Internet can be seen by others
- Always show respect and be polite to others when you are online.
- Be aware that information on a website may be inaccurate or biased. Try to verify the information using other sources, if possible, before using it
- Respect copyright and trademarks. You must not copy text or pictures from the Internet and hand it in to your teacher as your own work
- Always tell your teacher or another adult if you ever see, hear, or read anything which makes you feel uncomfortable while using the Internet or e-mail
- Always check with a supervisor before taking the following actions:
    - downloading files
    - completing questionnaires or subscription forms
    - opening e-mail attachments

You must not:

- Access chat rooms or personal websites
- Use or send bad, threatening, or annoying language
- Post anonymous messages or forward chain letters
- Use school computers for gambling, political purposes, or advertising.
- Interfere with another student's work
- Intentionally waste resources
- Access or send inappropriate materials such as pornographic, racist, or offensive material
- Access games

Please note:

- You should always log out when your session has finished
- All computers will be closely monitored, and staff may review your files and communications to maintain system integrity
- All Internet activity should be appropriate to your education
- Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate

THE VINE CHRISTIAN SCHOOL
Independent School - Ages 3 to 18

Student under 13 years old Acceptable Use and e-Safety Agreement

Parents, please read this with your child and tick to show you have done this, then sign on behalf of your child below:

- ☐ I will only use ICT in school for school purposes
- ☐ I will only use my class e-mail address or my own school e-mail address when e-mailing
- ☐ I will only open e-mail attachments from people I know, or who my teacher has approved
- ☐ I will not tell other people my ICT passwords
- ☐ I will only open/delete my own files
- ☐ I will make sure that all ICT contact with other children and adults is responsible, polite, and sensible
- ☐ I will not look for, save, or send anything that could be unpleasant or nasty. If I accidentally find anything like this, I will tell my teacher immediately
- ☐ I will not give out my own/others details such as name, phone number or home address. I will not arrange to meet someone or send my image unless this is part of a school project approved by my teacher and a responsible adult comes with me
- ☐ I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe
- ☐ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- ☐ I know that my use of ICT can be checked and my parent/carer contacted if a member of school staff is concerned about my safety
- ☐ I will not sign up for any online service unless this is an agreed part of a school project approved by my teacher
- ☐ I will not bring a Smart Watch to school because I am not allowed to wear one during the school day
- ☐ I will not sign up to online services like Facebook and Instagram

Signature …… (Parent /Carer) Date ……

Parent Name ……Student name…….....

THE VINE CHRISTIAN SCHOOL
Independent School - Ages 3 to 18

Student over 13 years old Acceptable Use Agreement / e-Safety Rules

Students, please read this with your parents and tick to show you have done this, then sign below:

- ☐ I will only use ICT systems in school, including the internet, e-mail, digital video, and mobile technologies for school purposes
- ☐ I will not download or install software using school technologies
- ☐ I will only log on to the school network, other systems and resources with my own username and password and I will not reveal my passwords to anyone else
- ☐ I will only use my school e-mail address
- ☐ I will make sure that all ICT communications with students, teachers or others is responsible and sensible
- ☐ I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use
- ☐ I will not browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material, I will report it immediately to my teacher
- ☐ I will not give out any personal information online such as name, phone number or address.
- ☐ I will not arrange to meet someone unless this is part of a school project approved by my teacher
- ☐ I am aware that when I take images of students and/ or staff that I must only store and use these for school purposes in line with school policy and must never distribute these outside the school network without the permission of all parties involved. This includes school breaks and all occasions when I am in school uniform or when otherwise representing the school
- ☐ I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, students or others distress or bring the school community into disrepute, including through uploads of images, video, sounds or texts
- ☐ I will support the school approach to online safety and not upload or add any images, video, sounds or text that could upset any member of the school community
- ☐ I will always respect the privacy and ownership of others' work on-line
- ☐ I will not attempt to bypass the internet filtering system
- ☐ I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers
- ☐ I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parent/carer may be contacted
- ☐ I will not bring a Smart Watch to school because I am not permitted to wear one during the school day
- ☐ If I can bring a mobile phone into school, I will keep it switched off and inside my school bag when I am on school premises
- ☐ I will not sign up to online social media services like Facebook and Instagram until I am old enough and my parents allow me to do so

Signature …… Date ……

Full Name ……..... (Printed)

THE VINE CHRISTIAN SCHOOL
Independent School - Ages 3 to 18

Parent/Carer Acceptable Use Agreement / Code of Conduct

Student's name:	
Parents' Declaration ☐ We give permission for our child to have access to the internet and to ICT systems at The Vine Christian School. ☐ We have read and agree to follow The Vine Christian School's acceptable use and e-Safety rules and to support the safe use of ICT at school. ☐ We give permission for our child to receive age appropriate e-safety training in school, covering ICT use both in and out of school. ☐ We understand that although the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that students will be safe when they use the internet and ICT systems, the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies. ☐ We understand that our child's activity on the school ICT systems will be monitored and that the school will contact us if they have concerns about any possible breaches of the Acceptable Use Policy. ☐ We will encourage our child to adopt safe use of the internet and digital technologies at home and will inform the school if we have concerns over our child's e-safety. ☐ We will not allow our child to bring any smart watches, tablets or other devices that can be connected to the internet into school. ☐ If we allow our child to take a mobile phone into school, we will ensure they understand it must always be switched off and kept inside their school bag when on school premises. ☐ We will not allow any text, image, sound or video to be published online or sent via electronic communications, by us or our child, that could upset or offend any member of the school community or bring the school name into disrepute. ☐ We will support the school's policy and prevent our child from signing up to social media services such as Facebook, Instagram, Snapchat whilst they are underage (13+ years in most cases). ☐ We will take responsibility to close online social media accounts if our child is underage and we or the school discover they have created such accounts.	
Student's **FATHER** or legal guardian:	Student's **MOTHER** or legal guardian:
Signature:	Signature:
Name in full:	Name in full:
Date:	Date:

Staff, Volunteer, Trustee, Governor and Visitor Acceptable Use Agreement / E-Safety / Code of Conduct

Introduction

ICT (including data) and the related technologies such as e-mail, the internet and mobile devices are an expected part of our daily working life in school. This policy is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are always expected to sign this policy and adhere to its contents. Any concerns or clarification should be discussed with Mrs. René Esterhuizen.

This Acceptable Use Policy is intended to ensure:

- that staff and volunteers will be responsible users and stay safe while using the internet and other communications technologies for educational, personal, and recreational use.
- that school systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that staff are protected from potential risk in their use of technology in their everyday work.
- that staff and volunteers will have good access to digital technology to enhance their work, to enhance learning opportunities for students learning and will, in return, expect staff and volunteers to agree to be responsible users.

Acceptable Use Policy Agreement

I understand that I must use school systems in a responsible way, to ensure that there is no risk to my safety or to the safety and security of the systems and other users. I recognise the value of the use of digital technology for enhancing learning and will ensure that students receive opportunities to gain from the use of digital technology. I will, where possible, educate the young people in my care in the safe use of digital technology and embed online safety in my work with young people.

For my professional and personal safety:

- I will follow requirements for data protection as outlined in the Online Safety and Data Protection Policy.
- I understand that the school will monitor my use of the school digital technology and communications systems.
- I understand that the rules set out in this agreement also apply to use of these technologies (e.g. laptops, email, etc.) out of school, and to the transfer of personal data (digital or paper based) out of school.
- I understand that the school digital technology systems are primarily intended for educational use and that I will only use the systems for personal or recreational use within the policies and rules set down by the school.
- I will not disclose my username or password to anyone else, nor will I try to use any other person's username and password. I understand that I should not write down or store a password where it is possible that someone may steal it.
- I will immediately report any illegal, inappropriate, or harmful material or incident, I become aware of, to the appropriate person.

I will be professional in my communications and actions when using school ICT systems:

- I will not access, copy, remove or otherwise alter any other user's files, without their express permission.

- I will communicate with others in a professional manner, I will not use aggressive or inappropriate language and I appreciate that others may have different opinions.
- I will ensure that when I take and / or publish images of others I will do so with their permission and in accordance with the school's policy on the use of digital / video images. I will not use my personal equipment to record these images unless I have permission to do so. Where these images are published (e.g. on the school website) it will not be possible to identify by name, or other personal information, those who are featured.
- Photographs must be kept securely and used appropriately, whether in school, taken off the school premises or accessed remotely
- Images of students and/ or staff will only be taken, stored, and used for professional purposes in line with school policy and with written consent of the parent, carer or staff member
- Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Head Teacher
- I will support the school approach to online safety and not upload or add any images, video, sounds or text linked to or associated with the school or its community'
- I will only use social networking sites in school in accordance with the school's policies.
- I will only communicate with students / students and parents / carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any on-line activity that may compromise my professional responsibilities.

The school has the responsibility to provide safe and secure access to technologies and ensure the smooth running of the school:

- When I use my mobile devices (laptops / tablets / mobile phones / USB devices etc.) in school, I will follow the rules set out in this agreement, in the same way as if I was using school equipment. I will also follow any additional rules set by the school about such use. I will ensure that any such devices are protected by up to date anti-virus software and are free from viruses.
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Twitter account, or any other social media link, to students
- I will not use personal email addresses on the school ICT systems.
- I will not open any hyperlinks in emails or any attachments to emails, unless the source is known and trusted , or if I have any concerns about the validity of the email (due to the risk of the attachment containing viruses or other harmful programmes)
- I will ensure that my data is regularly backed up, in accordance with relevant school policies.
- I will not try to upload, download or access any materials which are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act) or inappropriate or may cause harm or distress to others. I will not try to use any programmes or software that might allow me to bypass the filtering / security systems in place to prevent access to such materials.
- I will not try (unless I have permission) to make large downloads or uploads that might take up internet capacity and prevent other users from being able to carry out their work.
- I will not install or attempt to install programmes of any type on a machine, or store programmes on a computer, nor will I try to alter computer settings, unless this is allowed in school policies.
- I will not disable or cause any damage to school equipment, or the equipment belonging to others.
- I will only transport, hold, disclose or share personal information about myself or others, as outlined in the School Personal Data Policy (or other relevant policy). Where digital personal data is transferred outside the secure local network, it must be encrypted. Paper based Protected and Restricted data must be held in lockable storage.
- I understand that data protection policy requires that any staff or student data to which I have access, will be kept private and confidential, except when it is deemed necessary that I am required by law or by school policy to disclose such information to an appropriate authority.
- I will immediately report any damage or faults involving equipment or software; however, this may have happened.

When using the internet in my professional capacity or for school sanctioned personal use:

- I will ensure that I have permission to use the original work of others in my own work

- Where work is protected by copyright, I will not download or distribute copies (including music and videos).

I understand that I am responsible for my actions in and out of the school:

- I understand that this Acceptable Use Policy applies not only to my work and use of school digital technology equipment in school, but also applies to my use of school systems and equipment off the premises and my use of personal equipment on the premises or in situations related to my employment by the school.
- I understand that if I fail to comply with this Acceptable Use Policy Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors / Directors and / or the Local Authority and in the event of illegal activities the involvement of the police.

User Signature

I have read and understand the above and agree to use the school digital technology systems (both in and out of school) and my own devices (in school and when carrying out communications related to the school) within these guidelines, and agree to the above Acceptable Use Agreement / E-Safety Rules

I understand this forms part of the terms and conditions set out in my contract of employment and agree to follow this code of conduct

Signature ……..…….…… Date ……

Full Name ……..... (Printed)

Job title ……

HELP AND SUPPORT

Our organisation has a legal obligation to protect sensitive information under the Data Protection Act 2018. For more information visit the website of the Information Commissioner's Office https://ico.org.uk/

The Information Management Toolkit for Schools is available at:
https://cdn.ymaws.com/irms.site-ym.com/resource/collection/8BCEF755-0353-4F66-9877-CCDA4BFEEAC4/2016_IRMS_Toolkit_for_Schools_v5_Master.pdf

Safeguarding Children online – free expert advice: http://www.getsafeonline.org

Review Online Safety policy and practice at https://360safe.org.uk/

Cloud (Educational Apps) Software Services and the Data Protection Act – Departmental advice for local authorities, school leaders, school staff and governing bodies, October 2015 – this is an advice and information document issued by the Department for Education. The advice is non-statutory, and has been produced to help recipients understand some of the key principles and their obligations and duties in relation to the Data Protection Act 2018 (the DPA), particularly when considering moving some or all of their software services to internet-based "cloud" service provision – https://www.gov.uk/government/publications/cloud-software-services-and-the-data-protection-act

Resources to support schools with online safety:

- Education for a Connected World framework from the UK Council for Child Internet Safety (UKCCIS)
- Guidance from the PSHE Association
- Be Internet Legends by Parent Zone and Google

Numerous organisations are listed in Annex C of KCSIE 2020, that can provide support concerning online safety

For additional help, email school.ictsupport@education.gsi.gov.uk

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 2018

The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants individual's rights of access to their personal data, compensation and prevention of processing. The **Data Protection Act 2018** implements the European Union's General Data Protection Regulation (GDPR) in national law.

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000

http://www.hmso.gov.uk/si/si2000/20002699.htm

Regulation of Investigatory Powers Act 2000

Regulating the interception of communications and making it an offence to intercept or monitor communications without the consent of the parties involved in the communication. The RIP was enacted to comply with the Human Rights Act 1998. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, however, permit a degree of monitoring and record keeping, for example, to ensure communications are relevant to school activity or to investigate or detect unauthorised use of the network. Nevertheless, any monitoring is subject to informed consent, which means steps must have been taken to ensure that everyone who may use the system is informed that communications may be monitored. Covert monitoring without informing users that surveillance is taking place risks breaching data protection and privacy legislation.

https://www.legislation.gov.uk/ukpga/2000/23

Human Rights Act 1998

https://www.legislation.gov.uk/ukpga/1998/42

OTHER ACTS RELATING TO ESAFETY

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

http://www.legislation.gov.uk/ukpga/2006/1

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of *Working Together to Safeguard Children, 2018* document as part of their child protection packs.

https://www.legislation.gov.uk/ukpga/2003/42

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence

liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent there is no need to prove any intent or purpose.

http://www.legislation.gov.uk/ukpga/2003/21/section/127

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

https://www.legislation.gov.uk/ukpga/1990/18

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

https://www.legislation.gov.uk/ukpga/1988/27

Copyright, Design and Patents Act 1988

Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the software licence.

https://www.legislation.gov.uk/ukpga/1988/48

Public Order Act 1986 (sections 17 – 29)

This Act makes it a criminal offence to stir up racial hatred by displaying, publishing or distributing written material which is threatening. Like the Racial and Religious Hatred Act 2006 it also makes the possession of inflammatory material with a view of releasing it a criminal offence.

https://www.legislation.gov.uk/ukpga/1986/64

Protection of Children Act 1978 (Section 1)

It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

https://www.legislation.gov.uk/ukpga/1978/37

Obscene Publications Act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

https://www.legislation.gov.uk/ukpga/Eliz2/7-8/66 and http://www.legislation.gov.uk/ukpga/1964/74

Protection from Harassment Act 1997

A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his course of conduct will cause the other so to fear on each of those occasions.

https://www.legislation.gov.uk/ukpga/1997/40

ACTS RELATING TO THE PROTECTION OF PERSONAL DATA

Data Protection Act 2018

http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Freedom of Information Act 2000

https://www.legislation.gov.uk/ukpga/2000/36

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/

COUNTER-TERRORISM AND SECURITY ACT 2015 (PREVENT), ANTI-RADICALISATION & COUNTER-EXTREMISM GUIDANCE

https://www.gov.uk/government/publications/preventing-extremism-in-schools-and-childrens-services

The school holds the document 'The Prevent duty Departmental Advice for Schools and Childcare Providers, June 2015' on file.