ONLINE AND E-SAFETY POLICY

This policy will be reviewed in full by the Governing Body on a bi-annual basis.

Signature …… Date ……

Early Years Manager at Carmel Christian School

Signature …… Date ……..

Chairperson of the Governing Body

Signature …… Date ……

Wayne Skinner, Chairperson CMI Board of Trustees

Revision table	Date	Details
Review	September 2018	Major rebuild of several sections
Review	21 August 2019	Review
Review	21 August 2020	Review
Review	8 October 2021	Review due to staff and setting changes
Next review due	8 October 2023	

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

- Safeguarding and Child Protection
- Data Protection
- Keeping Children Safe in Education, September 2021
- Teaching Online Safety in School, June 2019

INTRODUCTION

At Carmel Christian School**,** we understand the responsibility to educate our pupils 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 fundamental part of our safeguarding and child protection measures. 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 in order 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 as a whole. Currently, the internet technologies children and young people are using both inside and outside of the classroom include:

- Websites
- Apps
- Email, 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 schools 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/governors and regular visitors [for regulated activities]) 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 staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

DATA PROTECTION

Carmel Christian School holds a separate Data Protection Policy, including GDPR.

MONITORING

Authorised ICT staff may inspect any ICT equipment owned or leased by the school at any time without prior notice. If you are in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact their department. Any ICT authorised staff member will be happy to comply with this request.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice, video or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain school business related information; to confirm or investigate compliance with school policies, standards and procedures; to ensure the effective operation of school ICT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 2018, or to prevent or detect crime.

ICT authorised staff may, without prior notice, access the email or voicemail account, where applicable, of someone who is absent in order to deal with any business-related issues retained on that account.

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 pupil 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's 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 period;
- 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 in order 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 pupils, 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 person in Carmel Ministries International, which incorporates Carmel Christian School is: the Data Protection Officer, Andrew Smallridge.

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

COMPUTER VIRUSES

- 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.
- 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.

The Local Authority guidance documents are listed below:

HGfL: School Admin: School Office: Data Protection and Freedom of Information

- Head teacher's Guidance – Data Security in Schools – Dos and Don'ts
- Staff Guidance – Data Security in Schools – Dos and Don'ts
- Data Security in Schools - Dos and Don'ts

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 read and signed the Acceptable Use Agreement.
- Staff keep all school related data secure. This includes all personal, sensitive, confidential or classified data.
- Staff avoid leaving any portable or mobile ICT equipment or removable storage media in unattended vehicles. Where this is not possible, they keep it locked out of sight.
- Staff always carry their portable and mobile ICT equipment or removable media as hand luggage, and keep it under their control at all times.
- It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents emailed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, 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 (Senior Information Risk Owner), 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 Joanne Collins

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.

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 our school is Joanne Collins

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 overwritten 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 and/or organisation who received the disposed item

* if personal data is likely to be held, the storage media will be overwritten 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 website
- 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 email within most schools is an essential means of communication for both staff and pupils. In the context of Carmel Christian School, emails should not be considered private. Educationally, emails can offer significant benefits including direct written contact between schools on different projects, be they staff-based or pupil-based, within school or international. We recognise that pupils need to understand the purpose of an email in relation to their age and how to behave responsible online.

Managing Email

- The school gives all staff and trustees/governors their own email account to use for all school business as a work-based tool. This is to protect staff/trustees/governors, minimise the risk of receiving unsolicited or malicious emails and avoids the risk of personal profile information being revealed.
- Staff and trustees/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, email 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 pupils, parents or conduct any school business using personal email addresses.
- 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.
- All emails should be written and checked carefully before sending, in the same way as a letter written on school headed paper.
- Staff sending emails to external organisations or parents are advised to cc. the Early Years Manager.
- Emails created or received as part of staff's school job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. They must therefore actively manage your email account as follows:

    - Delete all emails of short-term value
    - Organise email into folders and carry out frequent house-keeping on all folders and archives
- Staff must inform the Early Years Manager if they receive an offensive email.
- In whatever way staff access their school email (whether directly, through webmail when away from the office or on non-school hardware) all the school email policies apply.

Sending Emails

- 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.*
- Use your own school email account so that you are clearly identified as the originator of a message.
- Keep the number and relevance of email 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 email is not to be used for personal advertising.

Receiving Emails

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

Emailing Personal, Sensitive, Confidential or Classified Information

Where staff conclude that email must be used to transmit such data, they must obtain the express consent from the Early Years Manager to provide the information by email. Exercise caution when sending the email and 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 absolutely 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.

E-SAFETY ROLES AND RESPONSIBILITIES

As e-safety is an important aspect of strategic leadership within the school, the Early Years Manager and Trustees/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 Joanne Collins who has been designated to 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.

Senior Management and Trustees/Governors are updated by the E-Safety Safeguarding Officer, and all Trustees/Governors have an understanding of 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 Agreement for staff, trustees/governors and visitors is to protect the interests and safety of the whole school community.

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 pupils 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 provides opportunities within a range of curriculum areas to teach about e-safety.
- Educating pupils about the online risks that they may encounter outside school is done informally when opportunities arise and as part of the e-safety curriculum.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- Our staff receive regular information and training on e-safety and how they can promote the 'Stay Safe' online messages.
- New staff receive information on the school's acceptable use agreements 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 (communicate with the DSL).

MANAGING THE SCHOOL E-SAFETY MESSAGES

- We endeavour to embed e-safety messages across the EYFS curriculum whenever the internet and/or related technologies are used.
- 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 Coordinator. 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 a racist incident.

A sample can be downloaded http://www.thegrid.org.uk/eservices/safety/incident.shtml

MISUSE AND INFRINGEMENTS

Complaints

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

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 DSL. Depending on the seriousness of the offence, sanctions could include immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Hertfordshire Flowcharts for managing an e-safety incident may be found at:
http://www.thegrid.org.uk/eservices/safety/incident.shtml

INTERNET ACCESS

The internet is an open worldwide communication medium, available to everyone, at all times. 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

- Staff will preview any recommended sites, online services, software and apps before use.
- All users must observe software copyright at all times. 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, pupils, 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.

Infrastructure

- Our school employs some additional web-filtering. However, the school will avoid internet filter 'over-block' as this may place 'unreasonable restrictions on what children can be taught'.
- Carmel 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 are aware that school-based email and internet activity can be monitored and explored further if required.
- The school does not allow pupils access to internet logs.
- 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.
- 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 there are any issues related to viruses or anti-virus software, the network manager should be informed.

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.

- Parents/carers are required to make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on the school website).
- The school disseminates information to parents relating to e-safety, where appropriate, in the form of:
    - Private Facebook page for parents
    - Newsletter items

PASSWORDS AND PASSWORD SECURITY

Passwords

- **Always use your own** personal passwords.
- Make sure you enter your personal passwords each time you log-on. Do not include passwords in any automated log-on procedures.
- Staff should change temporary passwords at first log-on.
- 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 colleague your password.**
- **If you aware of a breach of security with your password or account, inform Joanne Collins 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 who have left the school are removed from the system within 48 hours.

If you think your password may have been compromised or someone else has become aware of your password report this to the Early Years Manager.

Password Security

Password security is essential for staff, particularly as they are able to access and use pupil data. Staff are expected to have secure passwords which are not shared with anyone.

- 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.
- 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 unauthorised 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 fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, 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 Hertfordshire grid:

http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

REMOTE ACCESS

All staff members are responsible for all activity via their remote access facility.

- Only use equipment with an appropriate level of security for remote access.
- To prevent unauthorised access to school systems, keep all access information such as telephone numbers, log-on 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.
- Protect school information and data at all times, 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

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. Guidance can be found here:
http://www.thegrid.org.uk/eservices/safety/research/index.shtml#safeuse

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.
- Staff are not permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. However, with the express permission of the Early Years Manager, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.

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 located in the personnel file.

Publishing Pupils' 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:

- Classroom use, such as displays
- Learning journals/records
- School publications, such as newsletters
- School website
- Local press/media
- Facebook (CCSEarlyYears)
- Annual school photograph

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.

Pupils' full names will not be published alongside their image and vice versa. Postal addresses of pupils 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.

Further information relating to issues associated with school websites and the safe use of images in schools may be found at:

http://www.thegrid.org.uk/schoolweb/safety/index.shtml

http://www.thegrid.org.uk/info/csf/policies/index.shtml#images

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.
- Images/films of children are stored on the school's network. Rights of access to this

material are restricted to the teaching staff within the confines of the school network or other online school resource.

Webcams and CCTV

- We do not use CCTV or 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)
- Webcams include any camera on an electronic device that is capable of producing video.

Further information relating to webcams and CCTV may be found at:
http://www.thegrid.org.uk/schoolweb/safety/webcams.shtml-

Video Conferencing

- Permission is sought from parents and carers if their children are involved in video conferences with end-points outside of the school.
- All pupils 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 Early Years Manager 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 from the parents of those taking part.

Additional points to consider:

- Participants in conferences offered by third-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.

Further information and guidance relating to video conferencing may be found at:

http://www.thegrid.org.uk/learning/ict/technologies/videoconferencing/index.shtml

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

School ICT Equipment

- As users of the school ICT equipment, staff are responsible for their 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 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 is used 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 staff save your data on a frequent basis to the school's network. Staff are responsible for the backup and restoration of any 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.
- On termination of employment, resignation or transfer, staff will return all school ICT equipment to the school. They must also provide details of all their system log-ons so that they can be disabled.
- It is the staff's responsibility to ensure that any information accessed from their 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 Early Years Manager:
    - 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 and 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 the car before starting the 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 general 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 up 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 pupil or parent/carer using their personal device unless in an emergency, e.g., on a school trip.
- Pupils are not allowed to bring personal mobile devices/phones to the setting.
- 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.

School-Provided mobile devices

- 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 the devices of any member of the school community
- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, only these devices should be used.
- Where the school provides a laptop for staff, only this device may be used to conduct school business outside of school.

SOCIAL MEDIA

Facebook, Twitter and other forms of social media are increasingly becoming an important part of our daily lives.

- Our school uses Facebook to communicate with parents and carers. Alison Carson (Chair of Governors) 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 during school hours.
- Staff and Trustees/Governors, pupils are aware that the information, comments, images and video they post online can be viewed by others, copied and stay online forever.
- Staff and Trustees/Governors are aware that their online behaviour should always be compatible with UK law.

SERVERS

Carmel 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 of time
- 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 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 we appoint to dispose of the equipment must provide a **written guarantee** that they will irretrievably destroy the data by multiple over writing the data.

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, EY Manager and Trustees/Governors.

Appendix 1: ACCEPTABLE USE AGREEMENT

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

Staff, Volunteer, Trustee/Governor and Visitor

Acceptable Use Agreement (E-Safety Code of Conduct)

Introduction

ICT (including data) and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this agreement and adhere to its contents at all times.

This Acceptable Use Agreement 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 pupils learning and will, in return, expect staff and volunteers to agree to be responsible users.

<u>Acceptable Use Agreement</u>

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 pupils 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 E-Safety Safety Policy 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 full 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 pupils 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 Early Years Manager.
- 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 parents/carers using official school systems. Any such communication will be professional in tone and manner.
- I will not engage in any online 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 (laptop/tablet/mobile phone/USB, 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 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 that are illegal (child sexual abuse images, criminally racist material, adult pornography covered by the Obscene Publications Act), 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's Data Protection 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 the 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, regardless of how 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 (or voluntary involvement) with the school.

- I understand that if I fail to comply with this Acceptable Use Agreement, I could be subject to disciplinary action. This could include a warning, a suspension, referral to Governors/Trustees and/or the Local Authority, and in the event of illegal activities, the involvement of the police.

I have read and understood the above, and I 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.

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 ……

Appendix 2: HELP AND SUPPORT

Please check Bristol Safeguarding Partnership for local advice*

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/

Advice on e-Safety* - http://www.thegrid.org.uk/eservices/safety/index.shtml

Further guidance* - http://www.thegrid.org.uk/info/dataprotection/index.shtml#securedata

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 on page 94 of KCSIE 2018, that can provide support concerning online safety

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

Appendix 3: 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.