Greater Grace School of Christian Education

Online (E-safety) Policy

This policy updates and replaces Online (E-safety) Policy v2 (Previously Internet Access Policy). It includes Acceptable Use Agreements for staff, trustees and volunteers/visitors, for parent/ carers and for Junior and Senior pupils.

The Data Protection Policy (including GDPR) should be read alongside this policy.

Greater Grace School is an independent Christian school with close links to Greater Grace Evangelical Church. All three full time staff have not only been DBS-checked, but have known each other in a professional capacity for 23 years since the school started, as well as in a personal capacity within the church before that. As a small school in every sense, currently registered for 14 pupils, we are in an unusual position in that we have the privilege of knowing these children and their families extremely well, especially those who also attend Greater Grace Evangelical Church.

While we take great care to avoid familiarity, the closeness that we have is an advantage that helps us safeguard our pupils and promote their well being. We are friendly and personal in an open and transparent way with each class and each individual without favouritism. We are especially vigilant when the need arises to work one-on-one, ensuring that we remain within sight and/or sound of another member of staff, for example, through a window or open door. We acknowledge that adults should be circumspect in their communications with children so as to avoid any possible misinterpretation of their motives. We proactively challenge any behaviour that could be misinterpreted, recognising that “It could happen here.”

Please keep in mind as you read this policy that it reflects these dynamics and our ethos as a Christian school.

This policy will be reviewed regularly, and in particular, when the dynamics change, e.g. if our school is registered for more than 14 pupils in the future, 20 or even 30, we will review and adapt this policy as necessary.

INTRODUCTION

ICT in the 21st Century is seen as an essential resource 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.

Information and Communications Technology covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast paced evolution of ICT 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
- 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 ICT, 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 Internet technologies and that some have minimum age requirements (13 years in most cases).

At Greater Grace School***,*** we understand the responsibility to educate our pupils on e-safety Issues; teaching them the appropriate behaviours and critical thinking skills to enable them to remain both safe and legal when using the internet and related technologies, in and beyond the context of the classroom.

Schools hold personal data on learners, staff (employees and volunteers) 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 our 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. Please read the Data Protection Policy.

Both this Online Policy and the Acceptable Use Agreements (for all staff, Trustees, regular visitors [for regulated activities] and pupils) 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 pupils and staff, but brought onto school premises (such as laptops, mobile phones and other mobile devices).

BREACHES

A breach or suspected breach of policy by a staff member, 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 Disciplinary Policy Procedure. 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 Motivation and Behaviour Management Policy.

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment or data (including remote access ID and PINs), and any unauthorised use or suspected misuse of ICT must be immediately reported to the relevant responsible person, Diane Bailey.
Please refer to the relevant section on Incident Reporting, e-safety Incident Log & Infringements below and to the Data Protection Policy.

COMPUTER VIRUSES

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

- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and contact Diane Bailey immediately so that our ICT support provider can advise you what actions to take and take responsibility 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. 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. Pupils are expected to keep their passwords private and not to share with others, particularly their friends.

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

- It is the responsibility of everyone to keep passwords secure

- Staff are aware of their responsibility to keep all school related data secure, and that particular care and attention must be given to all personal, sensitive, confidential or classified data. See relevant sections.

- Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. 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 keep it under your control at all times

- Pupils are only permitted to access their own files on the school network or local storage devices, and must not access the files of their peers, teachers or others.

- We recommend that staff lock the screen before leaving the computer unattended.

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

- We recommend that passwords contain a minimum of six characters and be difficult to guess, e.g. by including upper and lowercase letters, numbers and symbols

- Great care must be taken if passwords or encryption keys need to be recorded, e.g. in an encrypted file

- **Never tell a child your password**

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

- **Change passwords** whenever there is any indication of possible system or password compromise (e.g. someone else has become aware of your password). **If so, inform Diane Bailey immediately.**

- User ID and passwords for staff and pupils who have left the school are removed from the system to prevent unauthorized 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.
- Ensure that portable media containing sensitive information, such as USB sticks, are removed 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 to sensitive information
- 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

- Store all removable media securely
- Ensure removable media is purchased with encryption
- Encrypt files containing personal, sensitive, confidential or classified data
- Securely dispose of removable media that may hold personal data
- Ensure hard drives no longer in use are stored securely or wiped clean

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 good practice.

- 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. A member of the senior leadership team will be appointed to be the SIRO who will have 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 Anne Mulligan.

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 is able to manage and address risks to the information and make sure that information handling complies with legal requirements.
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 Anne Mulligan

MANAGEMENT OF ASSETS

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

  If personal data is likely to be held the storage media will be over written multiple times to ensure the data is irretrievably destroyed. A written guarantee will be obtained if any outside agency is appointed to dispose of equipment on the school's behalf.

- **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 **–** data protection guide, including the 8 principles

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

  Electricity at Work Regulations 1989
  http://www.opsi.gov.uk/si/si1989/Uksi_19890635_en_1.htm

Further information available on the **Environment Agency** web site
and the **Information Commissioner** Website https://ico.org.uk/

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 not only an invaluable resource for education, business, and social interaction, but also a potential risk to young and vulnerable people.

MANAGING THE INTERNET

- The school provides pupils with age appropriate supervised access to Internet resources through the school's fixed and mobile internet connectivity
- Staff will preview software, online services, and apps before use. Whenever appropriate, they will preview recommended sites before use
- Extra care is recommended when searching for images through open search engines when working with pupils
- If a homework project requires Internet research, parents will be reminded to supervise any Internet research by pupils in year 9 or lower.
- Supervision of Internet research at home by pupils in year 10 and above is at the parents' discretion.
- 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 or disseminate personal, sensitive, confidential or classified information in any way that may compromise the intended restricted audience
- Do not reveal names of 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

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

INFRASTRUCTURE

- Our school employs some additional web-filtering which is the responsibility of Anne Mulligan on behalf of the school's network manager
- Greater Grace School is aware of its responsibility when monitoring staff communication under current legislation and takes into account; 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 pupils are aware that school based e-mail and internet activity can be monitored and explored further if required
- The school does not allow pupils access to internet logs
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the teacher. The e-safety co-ordinator will be informed as soon as possible, and the incident will be logged
- 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

- Pupils 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 pupils wish to bring in work on removable media it must be given to Diane Bailey for a safety check first

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

- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head Teacher

MANAGING OTHER ONLINE TECHNOLOGIES

Online technologies if used responsibly (including social networking sites) 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 pupils 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 pupils within school

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

- Our pupils are advised to set and maintain their online profiles to maximum privacy and deny access to unknown individuals

- Pupils are always reminded to avoid giving out personal details which may identify them or where they are (full name, address, phone numbers, e-mail, school details)

- Pupils are encouraged to be wary about publishing specific and detailed private thoughts and information online and details of specific hobbies/ interests

- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such websites and to ensure that any images they post are appropriate due to the difficulty of removing an image once online

- Our pupils are asked to report any incidents of Cyberbullying to Diane Bailey

- Staff may create blogs, wikis or other online areas in order to communicate with pupils over 13 provided that their parents and the Head Teacher are aware

- Services such as Facebook and Instagram have a 13+ age rating which should not be ignored http://www.coppa.org/comply.htm

E-MAIL

The use of e-mail within most schools is an essential means of communication for both staff and pupils. 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 pupil based, within school or international.

We recognise that pupils need to understand how to style an e-mail in relation to their age and how to behave responsibly online.

- It is the responsibility of each account holder to keep the password secure
- 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 pupils are advised to cc the Head Teacher using greatergraces@gmail.com
- It is recommended that all staff & trustees have their own e-mail account to use for all school business. This is to protect staff, minimise the risk of receiving unsolicited e-mails and avoids the risk of personal profile information being revealed
- Wherever possible, staff & trustees should then use their school e-mail for all professional communication. School e-mails sent from personal accounts can be copied to the Head Teacher as above.
- Pupils are introduced to e-mail as part of the Computing Programme of Study
- All pupil e-mail users are expected to behave responsibly online and to adhere to the Acceptable Use Agreement appropriate to their age, particularly in relation to the use of appropriate language and to not revealing any personal details about themselves or others or arranging to meet anyone without specific permission
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive or upsetting e-mail. This should then be logged by the e-safety co-ordinator
- Staff are advised to inform the e-safety co-ordinator, Diane Bailey, if they receive an offensive e-mail on any school e-mail account so that it can be logged
- The forwarding of chain e-mails is not permitted in school
- However you access your school e-mail in or out of school, all the school e-mail policies apply

SENDING E-MAILS

- Refer to the Section ***E-MAILING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION*** before sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties
- Use your own school e-mail account as above 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 appropriate and necessary
- 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-MAILS

- Check your e-mail regularly
- It is recommended that you activate your ‘out-of-office’ notification when away for

extended periods

- Never open attachments from an untrusted source; seek advice if necessary
- Do not use the e-mail systems to store attachments. Detach and save business related work to the appropriate shared drive/folder wherever possible

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.**

It is recommended that you always follow these checks before releasing the e-mail.

- Encrypt and password protect.
- Verify (by phoning) the details of the requestor, the exact information required, and the reason, before responding to e-mail requests for information.
  Consider whether their request for **that** information is justified?
  If so, obtain express consent from your Head Teacher to send it by e-mail
- Verify the accuracy of the e-mail address of any intended recipient of the information
- Do not send the information to any person whose details you have been unable to separately verify (usually by phone)
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary
- 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: PUPILS WITH ADDITIONAL NEEDS

The school endeavours to create a consistent message with parents for all pupils and this in turn should inform future development of the school's e-safety rules. However, staff should be aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety issues. Where a pupil 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 and Trustees have ultimate responsibility to ensure that the policy and practices are embedded and monitored.

The member of the senior management team designated the e-safety co-ordinator is Diane Bailey. All members of the school community will be made aware of who holds this post.

It is the role of the e-safety co-ordinator 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 will be updated by the e-safety co-ordinator so that both 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 agreements for staff, Trustees, visitors and pupils, 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 in an age appropriate way. 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.

- Educating pupils about the online risks that they may encounter in and outside school is done informally when opportunities arise and as part of the Computing lessons

- Pupils are taught to critically evaluate materials and learn good searching skills through cross curricular teacher models and discussions

- Pupils are taught about copyright, respecting other people's information (e.g. referencing), safe use of images, relevant legislation that is there to protect them, and other important areas through discussion, modeling and appropriate activities

- Pupils are aware of the impact of Cyberbullying and know how to seek help if they are affected by any form of online bullying. Pupils are encouraged to seek help from a teacher/ trusted adult in school and to talk with their parent/ carer at home

- Pupils are also aware that they can seek advice or help from organisations such as Cybermentors, Childline, and the NSPCC, if they experience problems when using the internet and related technologies. They can also use the CEOP report abuse button

Information and support
There is a wealth of additional information available to support schools, colleges and parents to keep children safe online. See KCSIE 2021 Annex D.

E-SAFETY SKILLS DEVELOPMENT FOR STAFF

- 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. A list of helpful websites will be compiled in the Staff Folder

- Safeguarding updates, including information and training on e-safety and how staff can promote the 'Stay Safe' online messages are given at staff meetings

- 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. In the event of misuse of technology by any member of the school community, staff must speak to Diane Bailey, the e-safety Co-ordinator and Designated Safeguarding Lead, as soon as possible. If there are serious concerns about a child's safety, any staff member can contact the Integrated Access and Referral Team refer directly on 0300 123 7047

MANAGING THE SCHOOL E-SAFETY MESSAGES

- The e-safety policy will be introduced to the pupils at the start of each school year to progressively build age appropriate knowledge, understanding and skills

- We endeavour to embed e-safety messages across the curriculum whenever the internet and/or related technologies are used. These will be complemented through school displays and e-safety posters

- Consideration will be given each year to participation in Safer Internet Day in February.

INCIDENT REPORTING, E-SAFETY INCIDENT LOG, & INFRINGEMENTS

INCIDENT REPORTING

Any security breaches or attempts, loss of equipment or data (including remote access ID and PINs), and any unauthorised use or suspected misuse of ICT, as well as virus notifications and unsolicited e-mails, must be immediately reported to the relevant responsible person, Diane Bailey, who will also advise the Information Asset Owner, Anne Mulligan, when necessary.

E-SAFETY INCIDENT LOG

All incidents will be recorded by the e-safety co-ordinator. Some incidents may also need to be recorded elsewhere if they relate to a cyberbullying, extremism or racist incident.

MISUSE AND INFRINGEMENTS

COMPLAINTS

Complaints and/ or issues relating to e-safety should be made to the e-safety co-ordinator or Head Teacher. 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 co-ordinator and logged
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the e-safety co-ordinator, and an investigation by the Head Teacher. 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 misuse or misconduct when they sign the relevant User Agreement

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 plan to 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 make a decision as to whether they consent to images of their child being taken and used in the public domain (e.g., on school website)

- The school disseminates information to parents relating to e-safety where appropriate through newsletters. This could also be in the form of:

    - Information evenings
    - Practical training sessions e.g. current e-safety issues
    - Posters
    - School website information

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:
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

- Wherever possible, the school camera should be used

- Staff are permitted to use personal digital equipment, such as mobile phones and cameras, to record images of pupils, this includes when on field trips. Images should be transferred to the school's network

- Pupils are not permitted to use personal digital equipment, including mobile phones and cameras, to record images of pupils, staff and others without advance permission from their teacher

- Pupils and staff must give due consideration in the light of the Acceptable Use Agreement 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 located in the personnel file

PUBLISHING PUPIL'S IMAGES AND WORK

On a child's entry to the school, all parents/carers will be asked to give written 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

- in display material that may be used within the school's communal areas

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

- recorded/ transmitted on a video or webcam

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

The consent form will be kept on record by the school. Parents or carers may withdraw permission, in writing, at any time. 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.

Pupils' names will not be published alongside their image and vice versa. E-mail and postal addresses of pupils will not be published. Pupils' 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 Cathy Craddock has authority to upload to the internet.

STORAGE OF IMAGES

- Images/ films of children are stored on the school's network and backup devices. One of which is kept offsite.

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

- Anne Mulligan and Cathy Craddock have the responsibility of deleting the images when they are no longer required

VIDEO CONFERENCING
If we use this technology in the future

- Permission will be sought from parents/ carers if their children are involved in video conferences with end-points outside of the school

- All pupils will be supervised by a member of staff when video conferencing

- 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 third party organisations may not be DBS 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

ICT EQUIPMENT

INCLUDING PORTABLE & MOBILE ICT EQUIPMENT AND REMOVABLE MEDIA

- It is recommended that the School logs ICT equipment issued to staff and records serial numbers as part of the school's inventory

- Equipment must be kept physically secure in accordance with this policy to be

covered for insurance purposes.

- 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
- Care must be taken before allowing visitors to plug their ICT hardware into the school network points.
- Ensure portable and mobile ICT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades
- 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
- 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
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

USE OF SCHOOL AND PERSONAL ICT EQUIPMENT

- All activities may be monitored in accordance with this policy
- You are responsible for your activity whether using school ICT equipment or any personal equipment that you utilise in school or for school business,
- 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 (e.g. on a laptop)
- 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. When considering storing or transferring personal or sensitive data, please refer to the relevant section:

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE **MEDIA**

- It is recommended that a time locking screensaver is applied to all machines. Any device/ user profile accessing personal data must have a locking screensaver
- The school is not responsible for the loss, damage or theft of any personal mobile device

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.

USE OF SCHOOL AND PERSONAL MOBILE DEVICES INCLUDING PHONES

- 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

- Where the school provides mobile technologies such as phones, laptops and iPads for offsite visits and trips, these devices should be used whenever possible

- Where the school provides a laptop for staff, this device should be used to conduct school business outside of school whenever possible

- The school allows staff to bring in personal mobile phones and devices for their own use. At their discretion, a member of staff may contact a parent/ carer using their personal device

- Whenever possible, the school phone should be used to contact pupils. However, if written permission has been given by the parent/ carer, staff may use their personal phone to contact pupils over 13, and be contacted by them, in ways that promote pupil well being e.g. on a field trip

- Pupils are allowed to bring personal mobile devices/phones to school, but can only access them when on Privilege, or when given permission by a teacher

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

- 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

TELEPHONE SERVICES

- Staff 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 school policies.

- School telephones are provided specifically for school business purposes and

personal usage is a privilege that can 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

- Follow the appropriate procedures in the event of receiving a telephone call containing a bomb threat.

REMOVABLE MEDIA

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

STORING/TRANSFERRING PERSONAL, SENSITIVE, CONFIDENTIAL OR CLASSIFIED INFORMATION USING REMOVABLE **MEDIA**

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/ carers and with pupils over 13 where written permission has been given by the parent/ carer

- If written permission has been given by the parent/ carer, staff may use their personal Facebook account to contact pupils over 13, and be contacted by them, in ways that promote pupil well being

- Cathy Craddock is responsible for all postings on these technologies and monitors responses from others

  Staff may access their personal social media accounts at their discretion.

- Staff are able to setup Social Learning Platform accounts, using their school e-mail address, in order to be able to teach pupils the safe and responsible use of Social Media

- Pupils are not permitted to access their social media accounts whilst at school unless permission is given (in exceptional circumstances) by the Head Teacher

- Staff, Trustees, pupils, 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, pupils, 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, pupils, parents and carers are aware that their online behaviour should at all times be compatible with UK law

SERVERS

Greater Grace 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 devices should be encrypted by appropriate software
- Data must be backed up regularly
- Backup devices must be securely stored in a fireproof container
- Back up media stored off-site must be secure

SYSTEMS AND ACCESS

In accessing to any ICT equipment or systems in school or for school business, you recognise your responsibility to represent the school well and to comply with all relevant UK law

- 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 into disrepute. This includes, but is not limited to, jokes, chain letters; 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

WRITING AND REVIEWING THIS POLICY

Staff and Trustees have been involved in making/ reviewing the e-safety Policy and ICT Acceptable Use Agreements through discussions. Senior pupils will be given an opportunity to be involved in reviewing it.

REVIEW PROCEDURE

There will be on-going opportunities for staff and Trustees to discuss

- any e-safety issue that concerns them with the e-safety co-ordinator
- any issue of data security that concerns them with the IAO
- relevant issues during staff and/or Trustee meetings

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

This policy will be reviewed every 2 years and consideration will be given to the implications for future whole school development planning.

This policy has been read and approved by the staff, Head Teacher, and Trustees.

Policy v3 Adopted by Trustees on:	25/09/2019
Policy Last Reviewed on:	2/09/2021
Policy Due for Review by:	30/09/2023

123. It is essential that children are safeguarded from potentially harmful and inappropriate online material. An effective whole school and college approach to online safety empowers a school or college to protect and educate pupils, students, and staff in their use of technology and establishes mechanisms to identify, intervene in, and escalate any concerns where appropriate.

124. The breadth of issues classified within online safety is considerable, but can be categorised into four areas of risk:

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

• **contact:** being subjected to harmful online interaction with other users; for example: peer to peer pressure, commercial advertising and adults posing as children or young adults with the intention to groom or exploit them for sexual, criminal, financial or other purposes'.

• **conduct:** personal online behaviour that increases the likelihood of, or causes, harm; for example, making, sending and receiving explicit images (e.g consensual and non-consensual sharing of nudes and semi-nudes and/or pornography, sharing other explicit images and online bullying; and

• **commerce** - risks such as online gambling, inappropriate advertising, phishing and or financial scams. If you feel your pupils, students or staff are at risk, please report it to the Anti-Phishing Working Group (https://apwg.org/).

125. Schools and colleges should ensure online safety is a running and interrelated theme whilst devising and implementing policies and procedures. This will include considering how online safety is reflected as required in all relevant policies and considering online safety whilst planning the curriculum, any teacher training, the role and responsibilities of the designated safeguarding lead and any parental engagement.

Online safety policy

126. Online safety and the school or college's approach to it should be reflected in the child protection policy. Considering the 4Cs (above) will provide the basis of an effective online policy. The school or college should have a clear policy on the use of mobile and smart technology. Amongst other things this will reflect the fact many children have unlimited and unrestricted access to the internet via mobile phone networks (i.e. 3G, 4G and 5G). This access means some children, whilst at school or college, sexually harass their peers via their mobile and smart technology, share indecent images consensually and non-consensually (often via large chat groups) and view and share pornography and other harmful content. Schools and colleges should carefully consider how this is managed on their premises and reflect in their mobile and smart technology policy and their child protection policy.

Remote learning

127. Where children are being asked to learn online at home the Department has provided advice to support schools and colleges do so safely: safeguarding in schools colleges and other providers and safeguarding and remote education. The NSPCC and PSHE Association also provide helpful advice:

• NSPCC Learning - Undertaking remote teaching safely during school closures

• PSHE - PSHE Association coronavirus hub

Filters and monitoring

128. Whilst considering their responsibility to safeguard and promote the welfare of children and provide them with a safe environment in which to learn, governing bodies and proprietors should be doing all that they reasonably can to limit children's exposure to the above risks from the school's or college's IT system. As part of this process, governing bodies and proprietors should ensure their school or college has appropriate filters and monitoring systems in place. Governing bodies and proprietors should consider the age range of their children, the number of children, how often they access the IT system and the proportionality of costs vs risks.

129. The appropriateness of any filters and monitoring systems are a matter for individual schools and colleges and will be informed in part, by the risk assessment required by the Prevent Duty. UK Safer Internet Centre: appropriate filtering and monitoring. The UK Safer Internet Centre has published guidance as to what "appropriate" filtering and monitoring might look like:

130. Support for schools when considering what to buy and how to buy it is available via the: schools' buying strategy with specific advice on procurement here: buying for schools.

Information security and access management

131. Education settings are directly responsible for ensuring they have the appropriate level of security protection procedures in place, in order to safeguard their systems, staff and learners and review the effectiveness of these procedures periodically to keep up with evolving cyber-crime technologies. Guidance on e-security is available from the National Education Network. In addition, broader guidance on cyber security including considerations for governors and trustees can be found at NCSC.GOV.UK.

Reviewing online safety

132. Technology, and risks and harms related to it, evolve and change rapidly. Schools and colleges should consider carrying out an annual review of their approach to online safety, supported by an annual risk assessment that considers and reflects the risks their children face. A free online safety self-review tool for schools can be found via the 360 safe website.

133. UKCIS has published Online safety in schools and colleges: Questions from the governing board. The questions can be used to gain a basic understanding of the current approach to keeping children safe online; learn how to improve this approach where appropriate; and find out about tools which can be used to improve the approach. It has also published an Online Safety Audit Tool which helps mentors of trainee teachers and newly qualified teachers induct mentees and provide ongoing support, development and monitoring.

134. When reviewing online safety provision, the UKCIS external visitors guidance highlights a range of resources which can support educational settings to develop a whole school approach towards online safety.

Information and support

135. There is a wealth of additional information available to support schools, colleges and parents to keep children safe online. A sample is provided at Annex D.

GREATER GRACE SCHOOL OF CHRISTIAN EDUCATION

PARENT / CARER ACCEPTABLE USE AGREEMENT FOR E-SAFETY

New technologies have become integral to the lives of children and young people in today's society, both within schools and in their lives outside school. The internet and other digital information and communications technologies are powerful tools, which open up new opportunities for everyone. These technologies can stimulate discussion, promote creativity and stimulate awareness of context to promote effective learning. Young people should have an entitlement to safe internet access at all times.

This Acceptable Use Policy is intended to ensure:

- that young people will be responsible users and stay safe while using the internet and other communications technologies for educational, personal and recreational use.
- that school ICT systems and users are protected from accidental or deliberate misuse that could put the security of the systems and users at risk.
- that parents and carers are aware of the importance of e-safety and are involved in the education and guidance of young people with regard to their online behaviour.

Greater Grace School will do their best to ensure that students will have good access to ICT to enhance their learning and will, in return, expect the students to agree to be responsible users. A copy of the Student Acceptable Use Agreement is attached to this permission form, so that parents / carers will be aware of the school expectations of the young people in their care.

Parents are requested to sign the permission form below to show their support of the school in this important aspect of the school's work.

Permission Form

Parent / Carers Name

Student Name

As the parent / carer of the above student, I give permission for my son / daughter to have access to the internet and to ICT systems at school.

I know that my son / daughter has signed an Acceptable Use Agreement and has received, or will receive, e-safety education to help them understand the importance of safe use of ICT – both in and out of school.

I understand that the school will take every reasonable precaution, including monitoring and filtering systems, to ensure that young people will be safe when they use the internet and ICT systems. I also understand that the school cannot ultimately be held responsible for the nature and content of materials accessed on the internet and using mobile technologies.

I understand that my son's / daughter's activity on the ICT systems will be monitored and that the school will contact me if they have concerns about their safety or about any possible breaches of the Acceptable Use Policy.

I will encourage my child to adopt safe use of the internet and digital technologies at home and will ensure that appropriate systems are in place at home to protect and support my child.

Signed Date

GREATER GRACE SCHOOL OF CHRISTIAN EDUCATION

E-safety Rules – Senior Student Acceptable Use Agreement

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) are **not** appropriate for use in school. All Internet activity should be appropriate to your education
- Be aware that your actions on the Internet can be seen by others
- Treat others as they would expect to be treated, e.g. show respect and be polite
- Be aware that information on an Internet 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
- Always log out when your session has finished

You must not:

- Access chat rooms/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 other student's work
- Intentionally waste resources
- Access or send inappropriate materials such as pornographic, racist or offensive material
- Access games without specific permission

Please note:

- All computers will be closely monitored and staff may review your files and communications to maintain system integrity.
- Failure to follow the code will result in loss of access and further disciplinary action may be taken if appropriate

I understand that these E-safety rules are to keep me safe and that if staff are concerned about my safety, they will contact my parents
I will follow the code of conduct in this Acceptable Use Agreement

Name _____ Date _____

Signed _____

GREATER GRACE SCHOOL OF CHRISTIAN EDUCATION

Acceptable Use of School Computers Agreement

E-safety Rules

- I will **only** use the computers in school in the ways that my teacher tells me I can
- I will **only** use the computers for lessons
- I will **not** tell other people my computer passwords
- I will save my work in my own files
- I will **only** open or delete my own files on the computer
- I will **only access the internet when my teacher asks me to**
- I will **only** access the websites that my teacher tells me to look at
- I will **never access the internet when my teacher is not in the room.**
- I will **always tell my teacher** if I ever see, hear or read anything which makes me feel uncomfortable while using the Internet or e-mail

- I know that information on websites – words and pictures – may not be true so when I am not sure, I will talk to my teacher who will help me check

- I know that what I say and do on the Internet can be seen by people that I don't know so I will be polite and kind but I will not give out my name, address, or phone number

- I know that these rules are to keep me safe so I will be sensible and follow them carefully

- I know that my use of the computer is checked by my teacher who will contact my parents if concerned about my safety

I agree to these E-safety Rules

Name _____ Date _____

Signed _____

GREATER GRACE SCHOOL

Trustee and Volunteer / Visitor
Acceptable Use Agreement / Code of Conduct

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 who assist the School are aware of their professional responsibilities when using any form of ICT, and that all are expected to sign this policy and adhere at all times to its contents.
Any concerns or clarification should be discussed with Anne Mulligan.

- I will only use the school's e-mail / Internet / Network and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher or Chair of Trustees
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will not give out my own personal details, such as mobile phone number, personal e-mail address, personal Facebook or Twitter account, or any other social media link, to pupils
- I will ensure that personal data is kept secure and is used appropriately. Personal data can only be taken out of school when authorised by the Head Teacher or Chair of Trustees. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Head Teacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support the school approach to online safety.
- Images, or video/sound recordings, of pupils will only be taken, stored and used for professional purposes in line with school policy
- Images, or video/sound recordings, of pupils will not be distributed outside the school network, or uploaded to the internet, without the permission of the parent/ carer, or Head Teacher
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher
- I will respect copyright and intellectual property rights
- I will support and promote the school's e-safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand this Acceptable Use Agreement forms part of the Code of Conduct, and that sanctions may be used if needed

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

Signature …….…… Date ……

Full Name ……..... (Printed)

Job title ……

GREATER GRACE SCHOOL

Staff Acceptable Use Agreement / Code of Conduct

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 paid staff are aware of their professional responsibilities when using any form of ICT.
All staff are expected to sign this policy and adhere at all times to its contents.
Any concerns or clarification should be discussed with Anne Mulligan.

- I will only use the school's e-mail / Internet / Network and any related technologies for professional purposes or for uses deemed acceptable by the Head Teacher or Chair of Trustees
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role
- I will ensure that personal data is kept secure and is used appropriately. Personal data can only be taken out of school when authorised by the Head Teacher or Chair of Trustees. Personal or sensitive data taken off site must be encrypted, e.g. on a password secured laptop or memory stick
- I will not install any hardware or software without permission of the Head Teacher
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory
- I will ensure that my online activity, both in school and outside school, will not bring the school, my professional reputation, or that of others, into disrepute
- I will support the school approach to online safety
- Images, or video/sound recordings, of pupils will only be taken, stored and used for professional purposes in line with school policy
- Images, or video/sound recordings, of pupils will not be distributed outside the school network, or uploaded to the internet, without the permission of the parent/ carer, or Head Teacher
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Head Teacher
- I will respect copyright and intellectual property rights
- I will support and promote the school's e-safety and Data Protection policies and help pupils to be safe and responsible in their use of ICT and related technologies
- I understand this Acceptable Use Agreement forms part of the Code of Conduct, and that sanctions may be used if needed
- I understand this forms part of the terms and conditions set out in my contract of employment

User Signature
I agree to follow this code of conduct and to support the safe and secure use of ICT throughout the school

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.

Information Commissioner's Office https://ico.org.uk/

School's toolkit is available - Record Management Society website – http://www.rms-gb.org.uk/resources/848

Test your online safety skills http://www.getsafeonline.org

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

For additional help, e-mail school.ictsupport@education.gsi.gov.uk

CURRENT LEGISLATION

ACTS RELATING TO MONITORING OF STAFF E-MAIL

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.
http://www.hmso.gov.uk/acts/acts2000/20000023.htm

Human Rights Act 1998

http://www.hmso.gov.uk/acts/acts1998/19980042.htm

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.

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 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.

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.

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.

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 licence.

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.

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.

Obscene Publications Act 1959 and 1964

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

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 conduct will cause the other so to fear on each of those occasions.

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://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