Online Safety Policy – Maranatha Christian School

Staff Responsible	Tom Price
Head Approved	Tom Price
Trustee Approved	Lara Morava

Version	Date	Head Review	Trustee Review	Status	Next Review
V1.0	Mar 2016	Mar 16	Mar 16	OK	
V2.0	Mar 17	Mar 17	Mar 17	Updated	
V3.0	Sept 17	Sept 17	Sept 17	Updated	
V4.0	Nov 17	Nov 17	Nov 17	Updated	
V5.0	Oct 18	Oct 18	Oct 18	Updated	
V6.0	Feb 20	Feb 20	Feb 20	Ok	Feb 21
V7.0	Sept 2020	Sept 2020	Sept 2020	Ok	Sept 2021
V8.0	Sept 2021	Sept 2021	Sept 2021	Updated	Sept 2022
V9.0	Sept 2022	Sept 2022	Sept 2022	OK	Sept 2023
V10.0	Sept 2023	Sept 2023	Sept 2023	OK	Sept 2024

Contents

- E-mail
- School website
- Learning platform
- Social networking

5. Data Security

- Strategic and operational practices
- Data transfer

6. Equipment and Digital Content

- Personal mobile phones and devices
- Digital images and video

7. Education at home

The following are held as separate documents:

Acceptable Use Agreement (Students)
Acceptable Use Agreement (Staff and Volunteers)

The following are also used as reference:

Search and Confiscation guidance from DfE
https://www.gov.uk/government/publications/searching-screening-and-confiscation
Protocol for responding to online safety incidents www.saferinternet.org.uk

1. Introduction and Overview

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

- Data Protection Policy, including GDPR
- Child Protection and Safeguarding Policy
- KCSIE 2023

All information related to personal information is covered in the Data Protection Policy.

'Keeping Children Safe in Education' is statutory guidance from the Department for Education issued under Section 175 of the Education Act 2002, Children Act 2004, the Education (Independent School Standards) Regulations 2014 and the Education (Non-Maintained Special Schools) (England) Regulations 2011.

Definition of safeguarding

In relation to children and young people, safeguarding and promoting their welfare is defined in KCSIE as:

- protecting children from maltreatment
- preventing impairment of children's health or development
- ensuring that children are growing up in circumstances consistent with the provision of safe and effective care
- taking action to enable all children to have the best outcomes.

Rationale

The purpose of this policy is to:

- set out the key principles expected of all members of the school community at Maranatha Christian School with respect to the use of ICT-based technologies
- safeguard and protect the children and staff of Maranatha Christian School
- assist school staff working with children to work safely and responsibly with the Internet and other communication technologies and to monitor their own standards and practice
- set clear expectations of behaviour and/or codes of practice relevant to responsible use of the Internet for educational, personal or recreational use
- have clear structures to deal with online abuse such as cyberbullying which are cross referenced with other school policies
- ensure that all members of the school community are aware that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- minimise the risk of misplaced or malicious allegations made against adults who work with students

Some areas that may be of risk for our school community are:

Content

- exposure to inappropriate content, including online pornography, ignoring age ratings in games (exposure to violence associated with often racist language), substance abuse
- lifestyle websites, for example pro-anorexia/self-harm/suicide sites/promoting sexually inappropriate activities
- hate sites, for example extremist militant religious sites promoting verbal, physical or psychological violence
- content validation: how to check authenticity and accuracy of online content

Contact

- grooming
- cyber-bullying in all forms
- identity theft (including 'frape' (hacking Facebook profiles)) and sharing passwords

Conduct

- privacy issues, including disclosure of personal information
- digital footprint and online reputation
- health and well-being (amount of time spent online (Internet or gaming))
- sexting (sending and receiving of personally intimate images) also referred to as SGII (self-generated indecent images)
- plagiarism and copyright infringement

Scope

This policy applies to all members of Maranatha Christian School community (including staff, students / pupils, volunteers, parents / carers, visitors, community users) who have access to and are users of school 's ICT systems, both in and out of Maranatha Christian School.

The Education and Inspections Act 2006 empowers Head teachers, to such extent as is reasonable, to regulate the behaviour of students / pupils when they are off the school site and empowers members of staff to impose disciplinary penalties for inappropriate behaviour. This is pertinent to incidents of cyber-bullying or other online safety incidents covered by this policy, which may take place out of school, but are linked to membership of the school. The 2011 Education Act increased these powers with regard to the searching for and of electronic devices and the deletion of data. In the case of both Acts, action can be taken over issues covered by the Discipline, Behaviour and Exclusion Policy.

Role	Key Responsibilities

Headteacher	• To take overall responsibility for online safety provision
	• To take overall responsibility for data and data security (SIRO)
	• To ensure the school uses an appropriate web filtering software programme to restrict internet access.
	• To be responsible for ensuring that staff receive suitable training to carry out their online safety roles and to train other colleagues, as relevant
	• To be aware of procedures to be followed in the event of a serious online safety incident.
	• takes day to day responsibility for online safety issues and has a leading role in establishing and reviewing the school online safety policies / documents
	• promotes an awareness and commitment to e-safeguarding throughout the school community
	• ensures that online safety education is embedded across the curriculum
	• To ensure that all staff are aware of the procedures that need to be followed in the event of an online safety incident
	• To ensure that an online safety incident log is kept up to date
	• facilitates training and advice for all staff
	• liaises with the Local Authority and relevant agencies
	• Is regularly updated in online safety issues and legislation, and be aware of the potential for serious child protection issues to arise from:
	  • sharing of personal data
	  • access to illegal / inappropriate materials
	  • inappropriate on-line contact with adults / strangers
	  • potential or actual incidents of grooming
	  • cyber-bullying and use of social media

Trustees	• To ensure that the school follows all current online safety advice to keep the children and staff safe • To approve the Online Safety Policy and review the effectiveness of the policy. This will be carried out by the Trustees / Trustees Sub Committee receiving regular information about online safety incidents and monitoring reports. • To support the school in encouraging parents and the wider community to become engaged in online safety activities • The role of the Online Safety Trustee will include: • regular review with the Head teacher (including online safety incident log, filtering / change control log)

Role	Key Responsibilities
Parent volunteer technician	• To report any online safety related issues that arises, to the online safety coordinator. • To ensure that users may only access the school's networks through an authorised and properly enforced password protection policy, in which passwords are regularly changed • To ensure that provision exists for misuse detection and malicious attack e.g., keeping virus protection up to date) • To ensure the security of the school ICT system • To ensure that access controls / encryption exist to protect personal and sensitive information held on school-owned devices; • the school's policy on web filtering is applied and updated on a regular basis; • that he / she keeps up to date with the school's online safety policy and technical information in order to effectively carry out their online safety role and to inform and update others as relevant; • that the use of the network / remote access / email is regularly monitored in order that any misuse / attempted misuse can be reported to the Headteacher for investigation / action / sanction. • To ensure appropriate backup procedures exist so that critical information and systems can be recovered in the event of a disaster. • To keep up-to-date documentation of the school's e-security and technical procedures.
Teachers	• To embed online safety issues in all aspects of the curriculum and other school activities • To supervise and guide pupils carefully when engaged in learning activities involving online technology (including, extra-curricular and extended school activities if relevant) • To ensure that pupils are fully aware of research skills and are fully aware of legal issues relating to electronic content such as copyright laws
All staff	• To read, understand and help promote the school's online safety policy and guidance • To read, understand, sign and adhere to the school staff Acceptable Use Agreement / Policy • To be aware of online safety issues related to the use of mobile phones, cameras and hand held devices and that they monitor their use and implement current school policies with regard to these devices • To report any suspected misuse or problem to the online safety coordinator

Role	Key Responsibilities
	• To model safe, responsible and professional behaviours in their own use of technology • To ensure that any digital communications with pupils should be on a professional level and only through school based systems, never through personal mechanisms, e.g. email, text, mobile phones etc.
Pupils	• Read, understand, sign and adhere to the Student / Pupil Acceptable Use Agreement • have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations • to understand the importance of reporting abuse, misuse or access to inappropriate materials • to know what action to take if they or someone they know feels worried or vulnerable when using online technology. • to know and understand school policy on the use of mobile phones, digital cameras and hand held devices. • To know and understand school policy on the taking / use of images and on cyber-bullying. • To understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school • To take responsibility for learning about the benefits and risks of using the Internet and other technologies safely both in school and at home • to help the school in the creation/ review of online safety policies
Parents/carers	• to support the school in promoting online safety and endorse the Parents' Acceptable Use Agreement which includes the pupils' use of the Internet and the school's use of photographic and video images • to read, understand and promote the school Pupil Acceptable Use Agreement with their children • to access the school website • to consult with the school if they have any concerns about their children's use of technology
External groups	• Any external individual / organisation will sign an Acceptable Use Agreement prior to using any equipment or the Internet within school

Communication:

The policy will be communicated to staff/pupils/community in the following ways:

- Policy to be posted on the school website / staffroom/ classrooms
- Policy to be part of school induction pack for new staff
- Acceptable use agreements discussed with pupils at the start of each year.
- Acceptable use agreements to be issued to whole school community, usually on entry to the school
- Acceptable use agreements to be held in pupil and personnel files

Handling complaints:

- The school will take all reasonable precautions to ensure online safety. However, owing to the international scale and linked nature of Internet content, the availability of mobile technologies and speed of change, it is not possible to guarantee that unsuitable material will never appear on a school computer or mobile device. The school cannot accept liability for material accessed, or any consequences of Internet access.

- Staff and pupils are given information about infringements in use and possible sanctions. Sanctions available include:
  - interview/counselling by teacher/ Head teacher;
  - informing parents or carers;
  - removal of Internet or computer access for a period, [which could ultimately prevent access to files held on the system, including examination coursework];
  - referral to Police

- Any complaint about misuse is referred to the Headteacher.
- Complaints of cyberbullying are dealt with in accordance with our Anti-Bullying Policy. Complaints related to child protection are dealt with in accordance with school / LSCB child protection procedures.

Review and Monitoring

- The school has an online safety coordinator (Head teacher) who will be responsible for document ownership, review and updates.
- The online safety policy will be reviewed annually or when any significant changes occur with regard to the technologies in use within the school.
- The online safety is current and appropriate for its intended audience and purpose.
- There is widespread ownership of the policy and it has been agreed by the staff and approved by Trustees. All amendments to the school online safety policy will be discussed in detail with all members of teaching staff.

2. Education and Curriculum

Pupil online safety curriculum

This school

- Has a clear, progressive online safety education programme as part of the Computing curriculum / PSHE curriculum. It is built on LSCB/ MCS Safeguarding. This covers a range of skills and behaviours appropriate to the students' age and experience, including:
    - to STOP and THINK before they CLICK
    - to develop a range of strategies to evaluate and verify information before accepting its accuracy;
    - to be aware that the author of a website / page may have a particular bias or purpose and to develop skills to recognise what that may be;
    - to know how to narrow down or refine a search;
    - [for older pupils] to understand how search engines work and to understand that this affects the results they see at the top of the listings;
    - to understand acceptable behaviour when using an online environment / email, i.e. be polite, no bad or abusive language or other inappropriate behaviour; keeping personal information private;
    - to understand how photographs can be manipulated and how web content can attract the wrong sort of attention;
    - to understand why on-line 'friends' may not be who they say they are and to understand why they should be careful in online environments;
    - to understand why they should not post or share detailed accounts of their personal lives, contact information, daily routines, location, photographs and videos and to know how to ensure they have turned-on privacy settings;
    - to understand why they must not post pictures or videos of others without their permission;
    - to know not to download any files – such as music files - without permission;
    - to have strategies for dealing with receipt of inappropriate materials;
    - [for older pupils] to understand why and how some people will 'groom' young people for sexual reasons;
    - To understand the impact of cyberbullying, sexting and trolling and know how to seek help if they are affected by any form of online bullying.
    - To know how to report any abuse including cyberbullying; and how to seek help if they experience problems when using the Internet and related technologies, i.e. parent or carer, teacher or trusted staff member, or an organisation such as ChildLine or the CLICK CEOP button.

- Plans Internet use carefully to ensure that it is age-appropriate and supports the learning objectives for specific curriculum areas.
- Will remind students about their responsibilities through an end-user Acceptable Use Agreement which every student will sign/will be displayed throughout the school/will be displayed when a student logs on to the school network.
- Ensures staff will model safe and responsible behaviour in their own use of technology during lessons.

- Ensures that when copying materials from the web, staff and pupils understand issues around plagiarism; how to check copyright and also know that they must respect and acknowledge copyright / intellectual property rights;
- Ensures that staff and pupils understand the issues around aspects of the commercial use of the Internet, as age appropriate. This may include risks in pop-ups; buying on-line; on-line gaming / gambling;

Staff and Trustee training

This school

- Ensures staff know how to send or receive sensitive and personal data and understand the requirement to encrypt data where the sensitivity requires data protection;
- Makes regular training available to staff on online safety issues and the school's online safety education program; annual updates
- Provides, as part of the induction process, all new staff [including those on university/college placement and work experience] with information and guidance on the online safety policy and the school's Acceptable Use Policies.

Parent awareness and training

This school

- Runs a rolling programme of advice, guidance and training for parents, including:
    - Introduction of the Acceptable Use Agreements to new parents, to ensure that principles of e-safe behaviour are made clear
    - Information leaflets; in school newsletters; on the school web site;
    - demonstrations, practical sessions held at school;
    - suggestions for safe Internet use at home;
    - provision of information about national support sites for parents.

3. Expected Conduct and Incident management

Expected conduct

In this school, all users:

- are responsible for using the school ICT systems in accordance with the relevant Acceptable Use Agreement which they will be expected to sign before being given access to school systems.
- need to understand the importance of misuse or access to inappropriate materials and are aware of the consequences
- need to understand the importance of reporting abuse, misuse or access to inappropriate materials and know how to do so

- should understand the importance of adopting good online safety practice when using digital technologies out of school and realise that the school's Online safety Policy covers their actions out of school, if related to their membership of the school
- will be expected to know and understand school policies on the use of mobile phones, digital cameras and hand held devices. They should also know and understand school policies on the taking / use of images and on cyber-bullying

Staff

- are responsible for reading the school's online safety policy and using the school ICT systems accordingly, including the use of mobile phones, and hand-held devices.

Students/Pupils

- should have a good understanding of research skills and the need to avoid plagiarism and uphold copyright regulations

Parents/Carers

- should provide consent for pupils to use the Internet, as well as other technologies, as part of the Acceptable Use Agreement form at time of their child's entry to the school
- should know and understand what the 'Rules of Appropriate Use' are and what sanctions result from misuse

Incident Management

In this school:

- there is strict monitoring and application of the online safety policy and a differentiated and appropriate range of sanctions, though the attitudes and behaviour of users are generally positive and there is rarely need to apply sanctions
- all members and its wider community are encouraged to be vigilant in reporting issues, in the confidence that issues will be dealt with quickly and sensitively, through the school's escalation processes.
- support is actively sought from other agencies as needed (e.g. the LSCB and UK Safer Internet Centre helpline) in dealing with online safety issues
- monitoring and reporting of online safety incidents takes place and contributes to developments in policy and practice in online safety within the school. The records are reviewed/audited and reported to the school's senior leaders, Trustees / LSCB
- parents / carers are specifically informed of online safety incidents involving young people for whom they are responsible.
- We will contact the Police if one of our staff or pupils receives online communication that we consider is particularly disturbing or breaks the law

4. Managing the ICT infrastructure

- **Internet access, security (virus protection) and filtering**

This school:

- Uses internet filtering software to protect students from accessing harmful material.
- Does not allow the students of Early Years direct access to the internet at any time.
- Is vigilant in its supervision of pupils' use at all times, as far as is reasonable, and uses common-sense strategies in learning resource areas where older pupils have more flexible access;
- Ensures all staff and students have signed an acceptable use agreement form and understands that they must report any concerns;
- Informs all users that Internet use is monitored;
- Informs staff and students that that they must report any failure of the filtering systems directly to the Head teacher or their supervisor;
- Makes clear all users know and understand what the 'rules of appropriate use' are and what sanctions result from misuse – through staff meetings and teaching programme;
- Provides advice and information on reporting offensive materials, abuse/ bullying etc. available for pupils, staff and parents
- Immediately refers any material we suspect is illegal to the appropriate authorities – Police and the LSCB.

To ensure the network is used safely, this school:

- Ensures staff read and sign that they have understood the school's Acceptable Use Agreement
- Makes clear that no one should log on as another user and makes clear that pupils should never be allowed to log-on or use teacher and staff logins as these have far less security restrictions and inappropriate use could damage files or the network;
- Requires all users to always log off when they have finished working or are leaving the computer unattended;
- Where a user finds a logged-on machine, we require them to always log-off and then log-on again as themselves. Requests that teachers and pupils do not switch the computers off during the day unless they are unlikely to be used again that day or have completely crashed. We request that they DO switch the computers off at the end of the day.
- Has set-up the network so that users cannot download executable files / programmes;
- Has blocked access to music/media download or shopping sites – except those approved for educational purposes;
- Scans all mobile equipment with anti-virus / spyware before it is connected to the network;

- Makes clear that staff are responsible for ensuring that any computer or laptop loaned to them by the school, is used solely to support their professional responsibilities and that they notify the school of any "significant personal use" as defined by HM Revenue & Customs.
- Maintains equipment to ensure Health and Safety is followed;
  e.g. projector filters cleaned by staff; equipment installed and checked by professional suppliers;
- Has integrated curriculum and administration networks, but access to the staff site is set-up so as to ensure staff users only can access this site;
- Makes clear responsibilities for the regular back up of academic and other management systems and important files;
- Follows ISP advice on Local Area and Wide Area security matters and firewalls and routers have been configured to prevent unauthorised use of our network;
- All computer equipment meets health and safety standards;
- Projectors are maintained so that the quality of presentation remains high;
- Reviews the school ICT systems regularly with regard to health and safety and security.

Password policy

- This school makes it clear that staff and pupils must always keep their password private, must not share it with others and must not leave it where others can find it;
- We require staff to use a STRONG password for access into the school computer system.
- We require staff to change their password into the system twice a year.

E-mail

Pupils:

- know that spam, phishing and virus attachments can make e mails dangerous.
- are taught about the safety and 'netiquette' of using e-mail both in school and at home i.e. they are taught:
  - not to give out their e-mail address unless it is part of a school managed project or to someone they know and trust and is approved by their teacher or parent/carer;
  - that an e-mail is a form of publishing where the message should be clear, short and concise;
  - that any e-mail sent to an external organisation should be written carefully and authorised before sending, in the same way as a letter written on school headed paper;
  - they must not reveal private details of themselves or others in e-mail, such as address, telephone number, etc.;
  - to 'Stop and Think Before They Click' and not open attachments unless sure the source is safe;
  - that they should think carefully before sending any attachments;

- not to respond to malicious or threatening messages;

- Pupils sign the school Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

Staff:

- Staff know that e-mail sent from school email address to an external organisation must be written carefully, (and may require authorisation), in the same way as a letter written on school headed paper.
- All staff sign the School Agreement Form to say they have read and understood the online safety rules, including e-mail and we explain how any inappropriate use will be dealt with.

School website

- The Trustees take overall responsibility to ensure that the website content is accurate and the quality of presentation is maintained;
- Uploading of information is restricted to our website authorisers
- The school website complies with the statutory DfE guidelines for publications;
- Most material is the school's own work; where other's work is published or linked to, we credit the sources used and state clearly the author's identity or status;
- The point of contact on the website is the school address, telephone number and we use a general email contact address, reception@maranathaschool.org. Home information or individual e-mail identities will not be published;
- Photographs published on the web do not have full names attached;
- We do not use pupils' names when saving images in the file names or in the tags when publishing to the school website;
- We do not use embedded geodata in respect of stored images

Social networking

- Teachers are instructed not to run social network spaces for student use on a personal basis or to open up their own spaces to their students, but to use the schools' preferred system for such communications.

School staff will ensure that in private use:

- No reference should be made in social media to students / pupils, parents / carers or school staff
- They do not engage in online discussion on personal matters relating to members of the school community
- Personal opinions should not be attributed to the school

CCTV

- We have CCTV in the school as part of our site surveillance for staff and student safety. We will not reveal any recordings to outside parties without permission except where disclosed to the Police as part of a criminal investigation.

5. Data security

Strategic and operational practices

At this school:

- The Head Teacher is the Data Protection Officer.
- All policy statements regarding the data protection of personal data are covered by the Data Protection Policy.
- Staff are clear who are the key contact(s) for key school information;
- We ensure staff know who to report any incidents to where data protection may have been compromised.
- All staff are DBS checked and records are held in one central record
- We ensure ALL the following school stakeholders sign an Acceptable Use Agreement form. We have a system so we know who has signed.
  - staff,
  - Trustees,
  - pupils
  - parents

  This makes clear staffs' responsibilities with regard to data security, passwords and access.
- For students who use school computers as a part of their education, files are not held on the local device but on the student's own one-drive account. This means that all the information is then backed up.
- For students who are provided with a <name>@maranathaschool.org email address, this must only be used for school-related activities.
- We follow LSCB guidelines for the transfer of any data, such as reports of children, to professionals working in the Local Authority or their partners in Children's Services / Family Services, Health, Welfare and Social Services.
- We ask staff to undertake at least annual house-keeping to review, remove and destroy any digital materials and documents which need no longer be stored.

6. Equipment and Digital Content

Personal mobile phones and mobile devices

- Mobile phones brought into school are entirely at the staff member, student's and parents' or visitors' own risk. The School accepts no responsibility for the loss, theft or damage of any phone or hand-held device brought into school.
- Student mobile phones which are brought into school must be turned off and given to the School Business Manager to be kept in the school office until the student leaves the premises.
- The recording, taking and sharing of images, video and audio on any mobile phone is to be avoided, except where it has been explicitly agreed otherwise by the Headteacher. Such authorised use is to be monitored and recorded. All mobile phone use is to be open to scrutiny and the Headteacher is to be able to withdraw or restrict authorisation for use at any time if it is to be deemed necessary.
- The School reserves the right to search the content of any mobile or handheld devices on the school premises (and by extension on school trips) where there is a reasonable suspicion that it may contain undesirable material, including those which promote pornography, violence or bullying. Staff mobiles or hand-held devices may be searched at any time as part of routine monitoring.
- No images or videos should be taken on mobile phones or personally-owned mobile devices without the prior consent of the person or people concerned.

Students' use of personal devices

- The School advises that student mobile phones should not be brought into school.
- The School accepts that there may be particular circumstances in which a parent wishes their child to have a mobile phone for their own safety when they leave the school premises.
- If a student breaches the school policy then the phone or device will be confiscated and will be held in a secure place in the school office. Mobile phones and devices will be released to parents or carers in accordance with the school policy.
- If a student needs to contact his or her parents or carers, they will be allowed to use a school phone.
- Students should protect their phone numbers by only giving them to trusted friends and family members. Students will be instructed in safe and appropriate use of mobile phones and personally-owned devices and will be made aware of boundaries and consequences.

Staff use of personal devices

- Staff are not permitted to use their own mobile phones or devices for contacting children, young people or their families within or outside of the setting in a professional capacity.
- Staff should not use personally-owned devices, such as mobile phones or cameras, to take photos or videos of students and will only use work-provided equipment for this purpose.
- If a member of staff breaches the school policy then disciplinary action may be taken.

Digital images and video

In this school:

- We do not identify pupils in online photographic materials or include the full names of pupils in the credits of any published school produced video materials / DVDs;

- Staff sign the school's Acceptable Use Agreement and this includes a clause on the use of mobile phones / personal equipment for taking pictures of pupils;
- If specific pupil photos (not group photos) are used on the school web site, in the prospectus or in other high profile publications the school will obtain individual parental or pupil permission for its long term use
- The school blocks/filter access to social networking sites or newsgroups unless there is a specific approved educational purpose;
- Pupils are advised to be very careful about placing any personal photos on any 'social' online network space. They are taught to understand the need to maintain privacy settings so as not to make public, personal information.
- Pupils are taught that they should not post images or videos of others without their permission. We teach them about the risks associated with providing information with images (including the name of the file), that reveals the identity of others and their location, such as house number, street name or school. We teach them about the need to keep their data secure and what to do if they are subject to bullying or abuse.

7. Education at home

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-collegesand-other-providers and safeguarding-and-remote-education

Appendix 1 – 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