"As unique individuals, we do our best at work and play for the love of God and others."

St Benedict's Catholic Primary School

E –Safety and Acceptable Use Policy

Adopted by St Benedict's Catholic Primary School: April 2020

Review Date: April 2023

Contents

E- Safety and Acceptable Use Policy

Introduction

Information and Communications Technology covers a wide range of resources and currently the internet technologies young people and adults are using both inside and outside of the classroom include:

- Websites
- Learning Platforms and Virtual Learning Environments
- E-mail and Instant Messaging
- Chat Rooms and Social Networking
- Blogs and Wikis
- Podcasting
- Video Broadcasting
- Music Downloading
- Gaming
- Mobile/ Smart phones with text, video and/ or web functionality
- Other mobile devices with web functionality

Much IT, particularly web-based resources, is not consistently policed. All users need to be aware of the range of risks associated with the use of such related technologies.

At St Benedict's we understand the responsibility to educate our pupils and staff on e-Safety issues; informing them about 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 teaching areas.

The School holds personal data on learners, staff and other people 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 damage to the reputation of the School.

Everybody in the School 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 are made aware of the risks and threats and how to minimise them.

This policy is inclusive of both the fixed and mobile internet; technologies provided by the School (such as PCs, laptops, personal digital assistants (PDAs), tablets, webcams, whiteboards, interactive projectors, voting systems, digital video equipment, etc); and technologies owned by pupils and staff,

but brought onto School premises (such as laptops, smart phones, smart watches and portable media players, etc).

Monitoring

Authorised IT staff may inspect any IT equipment owned or leased by the School at any time without prior notice. IT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without consent, to the extent permitted by law. This may be to confirm or obtain School business related information; to confirm or investigate compliance with School policies, standards and procedures; to ensure the effective operation of School IT; for quality control or training purposes; to comply with a Subject Access Request under the Data Protection Act 1998, or to prevent or detect crime.

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

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

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

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School IT hardware, software or services from the offending individual.
Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure or, where appropriate, the LA Disciplinary Procedure or Probationary Service Policy.
Policy breaches may also lead to criminal or civil proceedings.

Incident Reporting

Any security breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of IT must be immediately reported to the School's eSafety Co-ordinators (ICT Lead, the Headteacher, the Deputy Headteacher) and the Network Manager. Additionally all security breaches,

lost/stolen equipment or data (including remote access PINs), virus notifications, unsolicited emails, misuse or unauthorised use of IT and all other policy non-compliance must be reported to the Network Manager and Headteacher.

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

Computer Viruses

All files downloaded from the Internet, received via e-mail or on removable media (e.g. USB Flash drive/CD) must be checked for any viruses using the School provided anti-virus software.

Pupils and staff must never interfere with any anti-virus software installed on School IT equipment.

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

If you suspect there may be a virus on any School IT equipment, stop using the equipment and contact IT Help immediately. The IT support provider will advise you what actions to take and be responsible for advising others who need to know

Data Security

The accessing and appropriate use of School data is something that the School takes very seriously. The School follows and adheres to the General Data Protection Regulations.

The School gives relevant staff access to its Management Information System, with a unique ID and password.

All removable storage holding sensitive data must be encrypted with a secure password.

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

When sending emails with attachments including personal, sensitive, confidential or classified data, the document must be password protected. Where possible, pupils will be referred to by initials and never their full name.

Staff must be aware of their responsibility when accessing School data.

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

Staff must keep all School related data secure. This includes all personal, sensitive, confidential or classified data.

Staff should avoid leaving any portable or mobile IT equipment or removable storage media in vehicles unattended. Where this is not possible, keep it locked and out of sight.

Staff who carry portable and mobile IT equipment or removable media must keep it under their control and ownership at all times.

It is the responsibility of each member of staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared photocopiers (multi-function print, fax, scan and copiers) are used.

E-Mail

The use of e-mail within St Benedict's Catholic Primary School is an essential means of communication for staff. In the context of the School, e-mail should not be considered private.

Managing e-Mail

The School gives all staff their own e-mail account to use for all School business as a work based tool. This is to minimise the risk of receiving unsolicited or malicious e-mails and avoids the risk of personal profile information being revealed

It is the responsibility of each account holder to keep the password secure. For the safety and security of users and recipients, all mail is filtered and logged; if necessary e-mail histories can be traced. The School email account must be the account that is used for all School business and all contact between all School staff

Under no circumstances should staff contact pupils, parents/carers or conduct any School business using personal e-mail addresses.

All e-mails should be written and checked carefully before sending, in the same way as a letter written on School headed paper

The forwarding of chain letters is not permitted in the School. If encountered, contact IT help but do not forward the letter.

Staff must inform the Network Manager, the Headteacher or the Deputy Headteacher if they receive an offensive e-mail

However you access your School e-mail (whether directly, through webmail when away from the School or on non-School hardware) all the School e-mail policies apply.

Sending e-Mails

If sending e-mails containing personal, confidential, classified or financially sensitive data to external third parties or agencies, refer to the Section emailing Personal, Sensitive, Confidential or Classified Information (see below).

Use your own School e-mail account so that you are clearly identified as the originator of a message.

Keep the number and relevance of e-mail recipients, particularly those being copied, to the minimum necessary and appropriate.

Do not send or forward attachments unnecessarily. Whenever possible, send the location path to the shared drive rather than sending attachments.

School e-mail is not to be used for personal advertising.

Receiving e-Mails

Check your e-mail regularly.

Activate your 'out-of-office' notification when away for extended periods.

Never open attachments from a non-trustworthy source; consult the Network Manager first.

Do not use the e-mail systems to store attachments. Detach and save to the appropriate shared drive/folder.

E-mailing Personal, Sensitive, Confidential or Classified Information

Assess whether the information can be transmitted by other secure means before using e-mail. E-mailing confidential data is not recommended and should be avoided where possible.

Where your conclusion is that e-mail must be used to transmit such data:

Exercise extreme caution when sending the e-mail concerning confidential information and always follow these checks before releasing the e-mail:

- Verify the details, including accurate e-mail address, of any intended recipient of the information.
- If in doubt, do not send.
- Verify (by phoning) the details of a requestor before responding to e-mail requests for information.
- Do not copy or forward the e-mail to any more recipients than is absolutely necessary.
- Use initials of pupils instead of full names.
- **Password protect any attached documents.**

eSafety

eSafety - Roles and Responsibilities

The named e-Safety co-ordinators in this School are the ICT Lead, the Headteacher, the Deputy Headteacher who have been designated this role. The School Governors also have responsibility to ensure that the policy and practices are embedded and maintained. All members of the School community have been made aware of who holds this post. It is the role of the ICT lead to keep abreast of current issues and guidance through organisations such as LEA, CEOP (Child Exploitation and Online Protection) and Childnet

The staff, pupils and Governors are updated by the ICT Lead and all Governors have an understanding of the issues and strategies at the School in relation to local and national guidelines and advice

This policy, supported by the School's Acceptable Use agreements for staff, pupils, governors and visitors, is to protect the interests and safety of the whole School community.

e-Safety in the Curriculum

It is essential for e-Safety that guidance is given to the pupils on a regular basis. E-Safety is embedded within the wider curriculum and the School community will look for new opportunities to promote e-Safety.

Educating staff and pupils on the dangers of technologies that maybe encountered outside School is done as part of the e-Safety curriculum within the structure of the wider curriculum.

Pupils are taught about copyright and respecting other people's information, images, etc through discussion, modelling and 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 also aware of where to seek advice or help if they experience problems when using the Internet and related technologies; i.e. parent/ carer, teacher/ trusted staff member, or an organisation such as CEOP or Childline.

Pupils are taught to critically evaluate materials and learn good searching skills through cross-curricular teacher models, discussions and via the wider curriculum.

e-Safety Skills Development for Staff

Our staff receive regular information and training on e-Safety issues in the form of INSET training and updates and the e-Safety Policy.

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

All staff have been made aware of individual responsibilities relating to the safeguarding of young people within the context of e-Safety and know what to do in the event of misuse of technology by any member of the School community.

All staff are encouraged to incorporate e-Safety activities and awareness within their curriculum areas.

Managing the School e-Safety Messages

We endeavour to embed e-Safety messages across the curriculum whenever the internet and/or related technologies are used.
The pupils' Code of Practice will be introduced to the pupils at the start of each School year.

Internet Access

The internet is an open communication medium, available to all, at all times. It is an invaluable resource for education, business and social interaction, as well as a potential risk to everyone.

Managing the Internet

The School pupils will have supervised access to Internet resources (where reasonable) through the School's fixed and mobile internet technology.

Staff must preview any recommended sites before use.

All users must observe software copyright at all times. It is illegal to copy or distribute School software or illegal software from other sources.

All users must observe copyright of materials from electronic resources.

Internet Use

Staff and pupils must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.

Don't reveal names of colleagues, pupils or any other confidential information acquired through the School on any social networking site or blog.

On-line gambling or gaming is not allowed.

Infrastructure

Staff and pupils are aware that the School based email 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 e-safety coordinators or a member of staff as appropriate.

It is the responsibility of the School, by delegation to the e-safety coordinators, 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 not the School's responsibility nor the Network Manager's to install and/or maintain virus protection on personal systems.

Pupils and staff are not permitted to download programs or files on the School based technologies without seeking prior permission from the Network Manager.

If there are any issues related to viruses or anti-virus software, the Network Manager must be informed via IT help.

If staff require a site that is normally blocked to pupils to be opened in an IT suite or on mobile internet devices, this must be emailed in advance to IT Help.

Managing Other Web 2 Technologies

Web 2, including social networking sites, if used responsibly 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.

All pupils are advised to be cautious about the information given by others on sites, e.g. users not being who they say they are.

Pupils are advised to adhere to the minimum age guidelines.

Pupils are taught to avoid placing images of themselves (or details within images that could give background details including school uniform) on such sites and to consider the appropriateness of any images they post due to the difficulty of removing an image once online.

Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (e.g. full name, address, mobile/ home phone numbers, School details, IM/ email address, specific hobbies/ interests).

Pupils are advised to set and maintain profiles on such sites to maximum privacy and deny access to unknown individuals.

Pupils are encouraged to be wary about publishing specific and detailed private thoughts online.

Pupils are asked to report any incidents of bullying to the School.

Staff may only create blogs, wikis or other web 2 spaces in order to communicate with pupils using the School Learning Platform or other systems approved by the e-Safety Coordinators (ICT Lead, Headteacher, Deputy Headteacher). We only permit the use of facebook engagement with pupils through the school facebook page and not through personal accounts. We may allow access to external blogging sites by individual approval and agreement to controls introduced to minimise opportunity for abuse.

Parental/carer 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 also to be aware of their responsibilities. We regularly inform parents/ carers about e-Safety and seek to promote a wide understanding of the benefits related to IT and associated risks.

Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their young person on admission to the School.

Parents/ carers are required to make a decision as to whether they consent to images of their

son/daughter being taken/ used in the public domain (e.g., on School website)

The School disseminates information to parents/carers relating to e-Safety where appropriate in the form of;

- Information evenings
- Website postings
- Newsletter items

Passwords and Password Security

Passwords

Always use your own personal passwords to access computer based services.

Make sure you enter your personal passwords each time you logon. Do not include passwords in any automated logon procedures.

Temporary passwords should be changed at first logon.

Change passwords whenever there is any indication of possible system or password compromise.

Do not record passwords on paper or in an unprotected file.

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

Passwords must contain a minimum of six characters including both letters and numbers and must be difficult to guess.

User ID and passwords for staff and pupils who have left the School are removed from the system within 6 weeks.

If you think your password may have been compromised or someone else has become aware of your password report this to IT Help

Password Security

Staff are expected to have secure passwords which are not shared with anyone. The pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils are regularly reminded of the need for password security.

All users read and sign an Acceptable Use Agreement/Code of Practice to demonstrate that they have understood the School's e-safety Policy and Data Security.

Pupils are not allowed to deliberately access on-line materials or files on the School network, of other pupils or any staff.

Staff are aware of their individual responsibilities to protect the security and confidentiality of School networks and SIMs systems including ensuring that passwords are not shared and are changed periodically.

All networked workstations have an automatic screen saver (password protected) set to 15 minutes.

However, all staff are advised to lock their workstation when leaving their PC unattended.

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 you lock your screen before moving away from your computer during your normal working day to prevent unauthorised access.

Ensure the accuracy of any personal, sensitive, confidential and classified information you disclose or share with others.

Ensure that personal, sensitive, confidential or classified information is not disclosed to any unauthorised person.

Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared photocopiers (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 labelling.

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

Ensure removable media is purchased with encryption.

Store all removable media securely.

Securely dispose of removable media that may hold personal data.

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

Safe Use of Images

Taking of Images and Film

Only with the written consent of parents/carers (on behalf of pupils), will the School permit the appropriate taking of images by staff and pupils with School equipment. Images may be shared on School's website/social media platforms only if written consent is provided by parents/carers.

Publishing Pupil's Images and Work

On a student's entry to the School, all parents/carers will be asked to give permission to use their son or daughter's work/photos in the following ways:

- on the School website
- on School social media platforms
- in the School prospectus and other printed publications that the School may produce for promotional purposes
- recorded/ transmitted on a video or webcam
- in display material that may be used in the School's communal areas
- in display material that may be used in external areas, i.e. exhibition promoting the School
- general media appearances, e.g. local/ national media/ press releases sent to the press highlighting an activity (sent using traditional methods or electronically)

The consent form is considered valid for the entire period that the student attends this School unless there is a change in the student's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc.

This consent form is considered valid after the young person has left the School, unless School is informed otherwise.

Parents/carers may withdraw permission, in writing, at any time. Consent has to be given by both parents/carers in order for it to be deemed valid.

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.

It is at the Headteacher's discretion who can upload photos to sites.

Storage of Images

Images/ films of young people are stored on the School's network.

Rights of access to this material are restricted to the staff and pupils within the confines of the School network.

Webcams in the School are only ever used for specific learning purposes.

Misuse of the webcam by any member of the School community will result in sanctions.

- Consent is sought from parents/carers and staff on joining the School, in the same way as for all images.

Video Conferencing

Permission is sought from parents and carers if their son/daughter is involved in video conferences.

Permission is sought from parents and carers if their son/daughter is involved in video conferences with end-points outside of the School.

All pupils are supervised by a member of staff when video conferencing.

All pupils are supervised by a member of staff when video conferencing with end-points beyond the School.

The School keeps a record of video conferences, including date, time and participants.

Approval from the e-Safety Coordinators is sought prior to all video conferences within School.

The School conferencing equipment is not set to auto-answer and is only switched on for scheduled and approved conferences.

No part of any video conference is recorded in any medium without the written consent of those taking part.

School IT Equipment including Portable & Mobile IT Equipment & Removable Media

School IT Equipment

As a user of IT, you are responsible for any activity undertaken on the School's IT equipment provided to you.

It is recommended that the School logs IT equipment issued to staff and pupils and records serial numbers as part of the School's inventory.

It is imperative that you save your data on a frequent basis to the School's network drive. You are responsible for the backup and restoration of any of your data that is not held on the School's network drive.
Personal or sensitive data should not be stored on the local drives of desktop PCs. If it is necessary to do so the local drive must be encrypted.

It is recommended that a time locking screensaver is applied to all machines. Any PCs etc accessing personal data must have a locking screensaver as must any user profiles.
Privately owned IT equipment should not be used on a School network. If this is essential, staff must consult the Network Manager who will implement the required procedures.
On termination of employment, resignation or transfer, staff must return all IT equipment to the Network Manager. You must also provide details of all your system log-ons so that they can be disabled.
It is your responsibility to ensure that any information accessed from your own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.

All IT equipment allocated to staff must be authorised by the appropriate Line Manager. Authorising Managers are responsible for:

- maintaining control of the allocation and transfer within their unit
- recovering and returning equipment when no longer needed

All redundant IT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and GDPR (GDPR).

Portable & Mobile IT Equipment

This section covers such items as laptops, PDAs and removable data storage devices. Please refer to the relevant sections of this document when considering storing or transferring personal or sensitive data.

All activities carried out on School systems and hardware will be monitored in accordance with the e-Safety and Acceptable Use Policy.

Staff must ensure that all School data is stored on School's network, and not kept solely on the laptop.

Equipment must be kept physically secure in accordance with this policy to be covered for insurance purposes. When travelling by car, best practice is to place the laptop in the boot of your car before starting your journey.

Synchronise all locally stored data, including diary entries, with the central School network server on a frequent basis.

Ensure portable and mobile IT equipment is made available as necessary for anti-virus updates and software installations, patches or upgrades.

The installation of any applications or software packages must be authorised by the IT support team, fully licensed and only carried out by your IT support.

In areas where there are likely to be members of the general public, portable or mobile IT equipment must not be left unattended and, wherever possible, must be kept out of sight.

Portable equipment must be transported in its protective case, if supplied.

Mobile Technologies

Personal Mobile Devices (including phones)

The School allows staff to bring in personal mobile phones and devices for their own use.

Pupils are not allowed to bring their own mobile phones in to school unless agreed with Headteacher and have permission from parent/carer.
If pupils bring their mobile device into school, it must be put in a locked case upon arrival and stored until the end of the school day.

If a staff member finds a phone belonging to a child that has not been locked away, this must be reported to the Headteacher immediately.

If a staff member finds a pupils' phone where an indecent image of a minor is on the screen, the phone must be switched off immediately and the Headteacher informed. The Headteacher must then report this to the appropriate authorities.

The School is not responsible for the loss, damage or theft of any personal mobile device.

The sending of inappropriate text messages between any member of the School community is not allowed.

Permission must be sought before any image or sound recordings are made on these devices by any member of the School community and if permission is granted, the recording must be deleted as soon as it can uploaded onto the School's Network.

Users bringing personal devices into School must ensure there is no inappropriate or illegal content on the device.

School Provided Mobile Devices

Permission must be sought before any image or sound recordings are made on the devices of any member of the School community.

Where the School provides mobile technologies such as iPads, laptops and PDAs for offsite visits and trips, only these devices should be used.

Where the School provides a laptop for staff, only this device may be used to conduct School business outside of School.

Removable Media

If storing/transferring personal, sensitive, confidential or classified information using Removable Media please refer to the section 'Storing/Transferring Personal, Sensitive, Confidential or Classified Information Using Removable Media'

The following guidelines must be adhered to:

only recommended removable media is to be used

all removable media is stored securely

removable media is disposed of securely by the IT support team

back up media stored off-site must be secure

Systems and Access

You are responsible for all activity on School systems carried out under any access/account rights assigned to you, whether accessed via School IT equipment or your own PC.

Do not allow any unauthorised person to use School IT facilities and services that have been provided to you.

Use only your own personal log-ons, account IDs and passwords and do not allow them to be used by anyone else.

Keep your screen display out of direct view of any third party when you are accessing personal, sensitive, confidential or classified information.

Ensure you lock your screen before moving away from your computer during your normal working day to protect any personal, sensitive, confidential or otherwise classified data and to prevent unauthorised access.

Ensure that you log-off from the PC completely when you are going to be away from the computer for a longer period of time.

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

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

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

Telephone Services

You may 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, LEA policies.

School telephones are provided specifically for School business purposes and personal usage is a privilege that will be withdrawn if abused.

Be aware that the laws of slander apply to telephone calls. Whilst a telephone call may seem to have a temporary and private existence it still qualifies as admissible evidence in slander law cases.

Ensure that your incoming telephone calls can be handled at all times.

Current Legislation

Acts Relating to Monitoring of Staff eMail

General Data Protection Regulation 2018

The guide to the General Data Protection Regulation contains: information about consent/ an explanation of rights under GDPR/ descriptions of special category and criminal offence data/ guidance on protecting

children's data

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

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 e-Safety

Keeping Children Safe in Education (KCSiE) 2019

Statutory guidance for schools and colleges on safeguarding children and safer recruitment.

https://www.gov.uk/government/publications/keeping-children-safe-in-education--2

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 "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

For more information www.teachernet.gov.uk

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 1998

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.

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 2004

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

Acts Relating to the Protection of Personal Data

General Data Protection Regulation 2018

https://www.gov.uk/government/publications/guide-to-the-general-data-protection-regulation

Data Protection Act 1998

http://www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_1

The Freedom of Information Act 2000

http://www.ico.gov.uk/for_organisations/freedom_of_information_guide.aspx

Staff E-Safety Accecptable Use Agreement Form

This form relates to the staff eSafety and Acceptable Use Policy (AUP), to which it is attached. Please complete the sections below to show that you have read, understood and agree to the rues included in the Acceptable Use Policy. If you do not sign and return this agrrement, access will not be granted to School IT systems.

I have read and understand the above and agree to follow these guidelines when:

- I use the School IT systems and equipment (both in and out of school)
- I use my own equipment in school e.g. mobile devices, PDAs, cameras etc
- I use my own equipment out of School in a way that is related to me being a member of this School e.g. communicating with other members of the School, accessing school e-mail, websites etc.

Name of employee _____

Signed _____ Date_____