E-safety and Data Security Policy

Approved Date	Sept 2018
Approved At	Governors - FGB
Amended	May 2021 Reviewed and updated to latest UK Data Protection Laws by Data Protection Officer.
Reviewed by Governors	Sept 2021
Date of Next Review	September 2023
Statutory	NO
Adopted from Bracknell Forest	NO

E-Safety Policy including Data Security

Schools hold personal data on learners, staff and other people to help them conduct their day-to-day activities. This may be electronic or as a hard copy. Some of this information is sensitive or confidential 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 undermine the data subject's perception of the school and make it more difficult for the school to use technology to benefit learners.

Everybody in our 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 should be made aware of the risks and threats and how to minimise them. This information may be in an electronic form or on paper.

Both this policy and the Acceptable Use Agreements (for all staff, governors, visitors, parents and pupils) are inclusive of both fixed and mobile internet; technologies provided by the school (such as PCs, laptops, tablets, datasticks, whiteboards, digital video equipment, etc); and technologies owned by staff, but brought onto school premises (such as laptops, mobile phones, camera phones, datasticks and portable media players, etc).

Monitoring

Authorised ICT staff employed by the school may inspect any ICT equipment owned or leased by the School at any time without prior notice.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, e-mails, 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 ICT; for quality control or training purposes; to comply with a Subject Access Request under the UK General Data Protection Regulation and Data Protection Act 2018, or to prevent or detect crime.

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

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

Please note that personal communications using School ICT may be unavoidably included in any business communications that are monitored, intercepted and/or recorded due to the schools' statutory obligations.

Breaches

A breach or suspected breach of policy by a School employee, contractor or pupil may result in the temporary or permanent withdrawal of School ICT hardware, software or services from the offending individual.

Any policy breach is grounds for disciplinary action in accordance with the School Disciplinary Procedure.

Policy breaches may also lead to criminal or civil proceedings.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously. The school Data Protection policy should be read in conjunction with this policy. Any data breach must be reported immediately to the Head (or Data Protection Officer if Head not available) to ensure that the authorities are informed within 72hours and the effect of any breach can be minimised.

All school data should be stored in a secure area on the school website or server, an encrypted password protected datastick or an encrypted password protected laptop only. It must never be stored on a laptop that is not encrypted, especially not on the desktop. Paper copies of data should not include contextual data e.g. date of births, ethnicity etc unless necessary and should be shredded once not required any longer.

All members of staff are expected to keep all school related data secure. This includes all personal, sensitive, confidential or classified data whether paper or electronically based.

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, this is also the case if the equipment is left on site overnight.

Staff should always carry portable and mobile ICT equipment or removable media as hand luggage, and keep it under your control at all times.

It is the responsibility of individual staff to ensure the security of any personal, sensitive, confidential and classified information contained in documents faxed, copied, scanned or printed. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and in turn this should be sent to the User Box function on the staff general copier only.

Anyone expecting a confidential/sensitive fax, should have warned the sender to notify before it is sent using the Safe Haven Fax procedure below:

Safe Haven Fax procedures

When sending personally identifiable information:

- ensure the recipient knows the fax is being sent.
- ensure the fax will be collected at the other end.
- send the front sheet through first.
- check that it has been received by the correct recipient.
- add the rest of the document to the fax.
- press the **redial** button.
- don’t walk away while transmitting.
- wait for the original to process and remove it from the fax machine.
- wait for confirmation of successful transmission.

- confirm whether it is appropriate to fax to another colleague if they are not there to receive it.

- use only the minimum information and anonymise where possible

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 College Town Primary 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/parent based.

- The school gives all administrative and teaching 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 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 should be the account that is used for all school business

- Under no circumstances should staff contact pupils, parents or conduct any school business using personal 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. For example:

    - **Do not use text language or informal language in school e-mails.**

    - **Always sign off with a name (and contact details if applicable).**

    - **Make sure that you use plain English and ensure that you have made it clear how you need the recipient to respond.**

    - **Never write a whole e-mail in capital letters.**

    - **Always spell check an e-mail before you send it. Do not use the urgent flag unless it is absolutely necessary, recipients will not respond to the urgent flag if they perceive that you use it routinely.**

    - **If possible, try to stick to one subject for the content of each e-mail, as it will be easier to categorise it later if you need to keep the e-mail.**

- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or in the case of emails relating to a person on request as a result of a Secure Access Request under the Data Protection regulations (GDPR.) You must therefore actively manage your e-mail account as follows:

    – Delete all e-mails of short-term value
    – Organise e-mail into folders and carry out frequent house-keeping on all folders and archives

- 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

- Ask yourself whether this transaction needs to be done by e-mail? It may be that it is more appropriate to use the telephone or to check with someone face to face. Limit recipients to the people who really need to receive the e-mail. Avoid the use of global or group address lists unless it is absolutely necessary.

- E-mail is primarily a communications tool, and e-mail applications are not designed for keeping e-mail as a record in a storage area meeting records management storage standards. Therefore where the main purpose of the e-mail is to transfer documents, then the documents should be saved to a secure location.

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 allowed.

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

    - Exercise caution when sending the e-mail 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
        - 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

- Do not send the information to any body/person whose details you have been unable to separately verify (usually by phone)
- Send the information as an encrypted document **attached** to an e-mail or via a secure email service.
- Provide the encryption key or password by a **separate** contact with the recipient(s) – preferably by telephone
- Do not identify such information in the subject line of any e-mail
- Request confirmation of safe receipt

In exceptional circumstances, the Local Authority makes provision for secure data transfers to specific external agencies. Such arrangements can be checked and confirmed with the appropriate body such as doctors, nurses and other health staff, education staff and social workers.

Managing the Internet

- As part of the Prevent agenda the school will ensure an effective filtering and monitoring system to prevent radicalization and access to extremist views.

- The filtering system will also ensure that inappropriate sites cannot be accessed e.g adult material; racist or anti-religious material; violence; promotion of drugs; illegal activity etc

- Students will have supervised access to Internet resources (where reasonable) through the school's fixed and mobile internet technology

- Staff will preview any recommended sites before use to ensure content is appropriate

- Raw image searches are discouraged when working with pupils- Google Safesearch is the recommended school search provider.

- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher and displayed on the class webpage. It is advised that parents recheck these sites and supervise this work. Parents will be advised to supervise any further research.

- 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.

- In the event of a child or adult receiving an abusive message or accidentally accessing a website that contains abusive or inappropriate material the material should be copied/stored and a copy sent to the headteacher. However the screen displaying the material should be closed down as soon as possible to avoid further offence. The incident will then be investigated by the school.

Internet Use

- You 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, students or parents or any other confidential information acquired through your job on any social networking site or blog (See the Staff Acceptable Use Policy Appendix 2)

Passwords and Password Security
Passwords

- Always use your own personal passwords to access computer based services. These must contain at least 8 characters which should contain at least one capital letter and one number.

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

- Staff should change temporary passwords at first logon.

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

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

- Only disclose your personal password to authorised ICT support staff when necessary, and never to anyone else.

- User ID and passwords for staff who have left the School are removed from the system within 2 weeks and a log is kept in the school office, as well as on the H drive in ICT (see appendix 5).

If you think your password may have been compromised or someone else has become aware of your password report this to the ICT support team

- All staff are aware of their individual responsibilities to protect the security and confidentiality of school networks, MIS systems and/or Learning Platform, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that workstations are not left unattended and are locked. The automatic log-off time for the school admin network is a maximum of 15 minutes.

- The SIMS administrator termly checks SIMS access rights. Staff who leave will be removed from the database within 2 weeks. New arrivals and leavers or any changes made to who can access SIMS are noted on the appropriate form and the form is then kept on the H drive. (See appendix 4). Similar practices are in place for users of the website, offsite visit databases and other password protected information (see appendix 5)

Personal or Sensitive Information

Protecting Personal, Sensitive, Confidential and Classified Information

- Ensure that any School information accessed from your own PC or removable media equipment is kept secure and printed copies are locked away overnight. The school office and confidential documents are locked overnight.

- Teaching staff are expected to lock their screen before moving away from their computer during their normal working day to prevent unauthorised access

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

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

- Ensure the security of any personal, sensitive, confidential and classified information contained in documents you fax, copy, scan or print. This is particularly important when shared copiers (multi-function print, fax, scan and copiers) are used and when access is from a non-school environment. Use user boxes to print to ensure documents are not left unattended after printing.

- 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 in accordance with the records management policy. If documents do not need to be retained these nuts be destroyed as soon as no longer needed. Information such as trackers can have contextual data such as ethnicity, date of births etc removed before printing.

Webcams and CCTV

- The school uses CCTV for security and safety. The CCTV recorder is password protected and can only be accessed by authorized personnel and the two CCTV

servers are locked in the school's comms cupboards in KS1 And KS2 respectively. The cameras are located at the entrances and exits to school, around the outside of the school buildings and also at key locations inside school, e.g. where the server is located. Images are retained for 30 days.

- The only people with access to the recorder are the Headteacher, Assistant Heads, School Business Manager, Office Administrator, Welfare & Attendance Officer and Site Controller. Notification of CCTV use is displayed at the front of the school. Please refer to the hyperlink below for further guidance https://ico.org.uk/media/1542/cctv-code-of-practice.pdf

- Webcams can be used in school for online meetings by staff. Staff should ensure that the meeting is either not being recorded or all personal taking part are aware and have approved the meeting to be recorded.
- Webcam use by pupils should not be allowed in school as standard practice. If it is required during times when outside agencies are not allowed to visit the school for one to one meeting with pupils, parental approval must be sort and a member of staff or parent must be present.
- Where an outside agency is not allowed to visit to deliver a lesson such as The Vikings, Birds of Prey and this is carried out online during the school lesson the webcam should not be on and pupils must not be visible to the presenter. If staff wish to introduce themselves via webcam at the start of the session this can be done but care must be taken that the pupils are not in view and the camera is turned off during the lesson/presentation.
- Misuse of the webcam by any member of the school community will result in sanctions (as listed under the ' inappropriate materials' section of this document)

Personal Mobile Devices (including phones)

- The school allows staff to bring in personal mobile phones and devices for their own use. Under no circumstances does the school allow a member of staff to contact a pupil or parent/ carer using their personal device

- Mobile phones for use around the school site or outside school are kept in the office. These must be requested well in advance so adequate charging of the devices, renewing of credit etc is organised. Staff may use their own personal phones on trips but they must only be used for phone calls relating to the school trip, not for taking photos or videos. Volunteers on school trips are asked not to take any photos of the children on their phones during the trip.

- Mobile phones which have a camera on them must be locked away during the school day when children are on premises. Lockers are provided for this for staff and visitors are asked to leave their phones at the office. Further details are available in the Staff Handbook and Child Protection Policy.

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

- As a user of ICT, you are responsible for any activity undertaken on the school's ICT equipment provided to you

- The school logs ICT equipment, serial numbers are recorded and this is updated at least yearly as part of the school's inventory

- Visitors are not allowed to plug their ICT hardware into the school network points (unless special provision has been made). They should be directed to the wireless ICT Facilities which are password protected where a guest access will be provided.

- All staff are expected to ensure that all ICT equipment that they use is kept physically secure

- Staff must 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 and could result in prosecution, by the Information Commissioner's Office, as an illegal act, and incur a custodial sentence.

- It is imperative that staff save their data on a frequent basis to the school's network drives as appropriate. They are responsible for the backup and restoration of any of their 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. Administrative staff should save their work to their personal secure areas on the H drive or their dedicated area on the server.

- It is recommended that a time locking screensaver is applied to all machines. Any admin PCs etc accessing personal data must have a locking screensaver as must any user profiles.

- Privately owned ICT equipment should not be used on the school network. The network is secure and attempts to access it will not be successful.

- On termination of employment, resignation or transfer, all ICT equipment is returned to the school.

- It is staff's responsibility to ensure that any information accessed from their own PC, tablet, mobile phone or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person

- Staff must ensure that all school data is stored on school's network, and not kept solely on the laptop. Any equipment where personal data is likely to be stored must be encrypted

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

- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act 2018(DPA2018)

- 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

- Any portable or mobile devices or removeable media, likely to contain personal data must be encrypted.

Servers and Back Up

- Newly installed servers holding personal data should be encrypted, therefore password protecting data.
- The server is located in the resource room in a purpose built server cupboard which includes air conditioning and is locked so that only authorized staff can access it. To further ensure the security of the server CCTV is installed in the room.
- We have limited access rights to ensure the integrity of the standard build
- The server is always password protected
- All servers have security software installed appropriate to the machine's specification
- The whole IT network including the data is backed up nightly between 9pm and midnight by the schools IT support company and stored off-site. A daily status email is sent to the IT supports back up team who monitor the status of the back up.
- Remote back ups are automatically securely encrypted.
- The school has full disaster recovery through the IT support company. If required IT would be able to either remove the infected server and download a clean copy of the system or install the system onto a new server within a day. Individual files can also be recovered and downloaded.
- The network is protected by anti-virus software provide by the IT support company which is regularly updated.
- Ensure that web browsers and other web based applications are operated at a minimum of 128 BIT cipher strength

Disposal of Redundant ICT Equipment Policy

- All redundant ICT equipment will be disposed of through an authorised agency only. This should include a written receipt for the item including an acceptance of responsibility for the destruction of any personal data
- All redundant ICT equipment that may have held personal data will have the storage media over written multiple times to ensure the data is irretrievably destroyed. Or if the storage media has failed it will be physically destroyed.
- 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

  The Data Protection Act 2018 and the UK General Data Protection Regulation (UK GDPR)

  https://ico.org.uk/for-organisations/guide-to-data-protection/

Electricity at Work Regulations 1989

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

- The school will maintain a comprehensive inventory of all its ICT equipment including a record of disposal
- The school's disposal record will include:
    - Date item disposed of
    - Authorisation for disposal, including:
        - verification of software licensing
        - any personal data likely to be held on the storage media? *
    - How it was disposed of e.g. waste, gift, sale
    - Name of person & / or organisation who received the disposed item

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

This policy and the Acceptable Use Policy are to be shared annually with staff, every September, and will be shared with new staff as part of their induction.

Appendix 1- Current Legislation adopted from Bracknell Forest LA

Legal Framework

Notes on the legal framework

This section is designed to inform users of potential legal issues relevant to the use of electronic communications. It is not professional advice and organisations should always consult with their legal team or the police.

Many young people and indeed some organisation staff and volunteers use the internet regularly without being aware that some of the activities they take part in are potentially illegal. Please note that the law around this area is constantly updating due to the rapidly changing nature of the internet.

Racial and Religious Hatred Act 2006

This Act makes 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.

Criminal Justice Act 2003

Section 146 of the Criminal Justice Act 2003 came into effect in April 2005, empowering courts to impose tougher sentences for offences motivated or aggravated by the victim's sexual orientation in England and Wales.

Sexual Offences Act 2003

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). This can include images taken by and distributed by the child themselves (often referred to as "Sexting"). A person convicted of such an offence may face up to 10 years in prison. The offence of grooming 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. (Typically teachers, social workers, health professionals, connexions staff etc fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape. N.B. Schools should have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child protection packs.

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.

Data Protection Act 2018 and UK General Data Protection Regulation
These data protection laws are considered jointly and require anyone who handles personal information to notify the Information Commissioner's Office of the type of processing it administers and must comply with important data protection principles when treating personal data relating to identified or identifiable individual. These laws also grant individuals rights, including the right of access, to their personal data, compensation, and prevention of processing, among others.

Privacy in Electronic Communications Regulations 2011
This data protection law requires anyone communicating using public electronic networks including websites, faxes, emails, and recorded telephone messages for either a service or promotional reason, to have a lawful basis to do so and evidence to support the action. In a maintained school setting this would normally only affect processes such as advertising school trips or events, administrating a school newsletter or parent association activities, or processing and communicating with parents on a school waiting list for a place for their child.

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 (e.g. using someone else's password to access files);
• gain unauthorised access, as above, in order to commit a further criminal act (such as fraud); or
• impair the operation of a computer or program (e.g. caused by viruses or denial of service attacks).
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 his or her "work" without permission. The material to which copyright may attach (known in the business as "work") must be the author's own creation and the result of some skill and judgement. It comes about when an individual expresses an idea in a tangible form. 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. It is an infringement of copyright to copy all or a substantial part of anyone's work without obtaining the 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.

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.

Regulation of Investigatory Powers Act 2000
The Regulation of Investigatory Powers Act 2000 (RIP) regulates the interception of communications and makes 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.

Criminal Justice and Immigration Act 2008
Section 63 offence to possess "extreme pornographic image"
63 (6) must be "grossly offensive, disgusting or otherwise obscene"
63 (7) this includes images of "threats to a person life or injury to anus, breasts or genitals, sexual acts with a corpse or animal whether alive or dead" must also be "explicit and realistic". Penalties can be up to 3 years imprisonment.

Education and Inspections Act 2006
Education and Inspections Act 2006 outlines legal powers for schools which relate to Cyberbullying/Bullying:
• Headteachers have the power "to such an extent as is reasonable" to regulate the conduct of pupils off site.
• School staff are able to confiscate items such as mobile phones etc when they are being used to cause a disturbance in class or otherwise contravene the school behaviour/anti-bullying policy

The Counter Terrorism and Security Act 2015
An Act to make provision in relation to terrorism; to make provision about retention of communications data, about information, authority to carry and security in relation to air, sea and rail transport and about reviews by the Special Immigration Appeals Commission against refusals to issue certificates of naturalisation; and for connected purposes.

Prevent Duty Guidance for England & Wales

Statutory guidance issued under section 29 of the Counter-Terrorism and Security Act 2015. Section 26 of the Counter-Terrorism and Security Act 2015 (the Act) places a duty on certain bodies ("specified authorities" listed in Schedule 6 to the Act), in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into

terrorism”. This guidance is issued under section 29 of the Act. The Act states that the authorities subject to the provisions must have regard to this guidance when carrying out the duty.

Appendix 2- Acceptable Use Policy- Staff, governors and visitors

COLLEGE TOWN PRIMARY SCHOOL
Acceptable Use Agreement: Staff, Governors and Visitors

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

The school has provided computers, tablets and other ICT equipment for use by staff, offering access to a vast amount of information and offering greater potential to support the curriculum. Equipment is provided and maintained for the benefit of all staff and you are encouraged to use and enjoy these resources, helping to ensure that they remain available for all.

1	I will only use the school's digital technology resources and systems for professional purposes or for uses deemed reasonable by the Head or Governing Body.
2	I will only use the approved secure email systems(s) for school business. I will ensure that all electronic communications with staff and pupils are compatible with my professional role. I will not conduct any school business using my personal e-mail address.
3	I will not browse, download or send material that could be considered offensive to colleagues or any other individuals
4	I will report any accidental access, receipt of inappropriate materials or filtering breaches to the school.
5	I will not allow unauthorised individuals to access my email/internet/networks or systems and I will not trespass into other users files or folders.
6	I will ensure that all my login credentials (including passwords) are not shared, displayed or used by any other individuals
7	I will not download any software or resources from the internet that can compromise the network or are not adequately licensed
8	I will follow the 'Guidance for Safer Working Practice for Adults who work with children and Young people in an education setting April 2020. https://c-cluster-110.uploads.documents.cimpress.io/v1/uploads/d2a90ef0-f98b-4fbb-a65c-9371d3706b04~110/original?tenant=vbu-digital
9	I will ensure that my personal email accounts, mobile/home telephone numbers are not shared with pupils or their families
10	I will not allow pupils to add me as a friend to their social networking site nor will I add them as a friend to my social networking site
11	I will ensure that any private social networking sites/blogs etc that I create or actively contribute to are not confused with my professional role
12	I understand that all internet and network usage can be logged and this information could be made available to the Head or Governing Body on request.
13	I will not connect a computer laptop or other device to the network that has not been approved by the school and meets the minimum security specification
14	I will respect copyright and intellectual property rights
15	I will not use personal digital cameras or camera phones for transferring images of pupils or staff.
16	I will follow the schools policy on taking, using and storing images of pupils and staff for school use. I will not distribute images outside the school network without the permission of the parent/carer.
17	I will not engage in any online activity that may compromise my professional responsibilities
18	I understand that the Data Protection Act requires that any information seen by me with regard to staff or pupils held within school will be kept private and confidential, except when it is deemed necessary that I am required by law to disclose such information to the appropriate authority

19	I will ensure any personal data I have access to is kept secure whether in school or taken off the premises and I will follow school policy when taking data off the premises. Any portable or mobile devices or removeable media, likely to contain personal data must be encrypted.
20	Any ICT I equipment I have signed for remains my responsibility until returned. I will avoid leaving any portable or mobile ICT equipment or removable storage media in untended vehicles. Where this is not possible I will keep, it locked out of sight. Please note your laptop is not insured left in your car.
21	I will at all times behave responsibly and professionally and will not publish any work-related content on the internet
22	I will ensure that I am aware of digital safeguarding issues so that they are appropriately embedded in my practice
23	I understand that failure to comply with this Acceptable Use Policy (AUP) could lead to disciplinary actions

Additional Information

Computer Viruses

- All files downloaded from the Internet, received via e-mail or on removable media (e.g. data stick, CD) must be checked for any viruses using school provided anti-virus software before using them.
- Never interfere with any anti-virus software installed on school ICT equipment that you use.
- You must regularly update your anti-virus software by connecting the laptop to the school network.
- If you suspect there may be a virus on any school ICT equipment, stop using the equipment and inform the IT support.

e-mail

- All e-mails should be written and checked carefully before sending, in the same way as a letter written on school headed paper
- E-mails created or received as part of your School job will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000 or a Subject Access Request under Data Protection and GDPR regulations. You must therefore actively manage your e-mail account as follows:
  - Delete all e-mails of short-term value
  - Organise e-mail into folders and carry out frequent house-keeping on all folders and archives
- Further information is in the E-Safety and Data Security Policy, available on the school website or from the School Office.

I understand that it is my responsibility to ensure that I remain up-to-date and read and understand the schools most recent Acceptable Use Policy (AUP).

I agree to follow this code of conduct and to abide by the schools most recent AUP.

Signature ……..…….…. Date ……..……

Full Name ……..(printed)

Job title ……

Equipment given (if applicable)	Serial Number	Signed for and dated	Returned Date
Laptop			
USB			
Camera			
IPad/Tablet			

College Town Primary School e-safety agreement form: parents

Please read the attached policies on the use of digital images and social networking and sign and return the slip at the bottom of the page by _____

Internet and ICT: As the parent or legal guardian of the pupil(s) named below, I grant permission for the school to give my *daughter / son* access to: ✔

- the Internet at school
- ICT facilities and equipment at the school.

I accept that ultimately the school cannot be held responsible for the nature and content of materials accessed through the Internet and mobile technologies, but I understand that the school takes every reasonable precaution to keep pupils safe and to prevent pupils from accessing inappropriate materials. ✔

I understand that the school can, if necessary, check my child's computer files and the Internet sites they visit at school and if there are concerns about my child's e-safety or e-behaviour they will contact me. ✔

Use of digital images, photography and video: I understand the school has a clear policy on "The use of digital images and video" and I support this. ✔

I understand that the school will use photographs of my child or including them in video material to support learning activities in school if permission has been given. ✔

I accept that the school may use photographs / video that includes my child in publicity that reasonably promotes the work of the school, and for no other purpose. ✔

I will not take and then share online, photographs of other children (or staff) at school events. ✔

Social networking and media sites: I understand that the school has a clear policy on "The use of social networking and media sites" and I support this. ✔

I understand that the school takes any inappropriate behaviour seriously and will respond to observed or reported inappropriate or unsafe behaviour. ✔

I will support the school by promoting safe use of the Internet and digital technology at home. I will inform the school if I have any concerns. ✔

ICT e-safety agreement form

My daughter / son name(s): _____

Parent / guardian signature: _____

Date: ___/___/___

The use of digital images and video

To comply with the Data Protection, Act 2018, we need your permission before we can photograph or make recordings of your daughter / son. This permission is sought on the admissions form completed before your child starts school. If you wish to change the permission please contact the school office.

We follow the following rules for any external use of digital images:

If the pupil is named, we avoid using their photograph.
If their photograph is used, we avoid naming the pupil.

Where showcasing examples of pupils work we only use their first names, rather than their full names.

If showcasing digital video work to an external audience, we take care to ensure that pupils aren't referred to by name on the video, and that pupils' full names aren't given in credits at the end of the film.

Staffs are only allowed to take photographs/videos using school equipment.

Examples of how digital photography and video may be used at school include:

- Your child being photographed (by the class teacher or teaching assistant) as part of a learning activity; e.g. taking photos or a video of progress made by a child, as part of the learning record, and then sharing with their parent / guardian.

- Your child's image being used for presentation purposes around the school; e.g. in class or wider school wall displays.

- Your child's image being used in a presentation about the school and its work in order to share its good practice and celebrate its achievements, which is shown to other parents, schools or educators; e.g. within a CDROM / DVD or a document sharing good practice; in our school prospectus or on our school website.
  In rare events, your child's picture could appear in the media if a newspaper photographer or television film crew attends an event.

Please note: If we, or you, actually wanted your child's image linked to their name we would contact you separately for permission, e.g. if your child won a national competition and wanted to be named in local or government literature.

The use of social networking and on-line media

This school asks its whole community, including parents and other relatives, to promote the 3 commons approach to online behaviour:

- **Common courtesy**
- **Common decency**
- **Common sense**

How do we show common courtesy online?

- We ask someone's permission before uploading photographs, videos or any other information about them online.
- *We do not write or upload 'off-hand', hurtful, rude or derogatory comments and materials. To do so is disrespectful and may upset, distress, bully or harass.*

How do we show common decency online?

- We do not post comments that can be considered as being **intimidating, racist, sexist, homophobic or defamatory. This is cyber-bullying** and may be harassment or libel.
- When such comments exist online, we do not forward such emails, tweets, videos, etc. By creating or forwarding such materials we are all liable under the law.

How do we show common sense online?

- We think before we click.
- We think before we upload comments, photographs and videos.
- We think before we download or forward any materials.
- We think carefully about what information we share with others online, and we check where it is saved and check our privacy settings.
- We make sure we understand changes in use of any web sites we use.
- We block harassing communications and report any abuse.

Any actions online that impact on the school and can potentially lower the school's (or someone in the school) reputation in some way or are deemed as being inappropriate will be responded to.

In the event that any member of staff, student or parent/carer is found to be posting libellous or inflammatory comments on Facebook or other social network sites, they will be reported to the appropriate 'report abuse' section of the network site.
(All social network sites have clear rules about the content which can be posted on the site and they provide robust mechanisms to report contact or activity which breaches this.)

In serious cases we will also consider legal options to deal with any such misuse.

The whole school community is reminded of the CEOP report abuse process:
https://www.thinkuknow.co.uk/parents/

Appendix 4- SIMS database users amendment form (located electronically in the H Drive under ICT) to be completed as applicable

SIMS DATABASE USERS - AMENDMENTS DATE:				
NEW USERS				
Forename	**Surname**	**Job Title**	**Reason**	**Email Address**
DELETED USERS				
Forename	**Surname**	**Job Title**	**Reason**	**Email Address**

Appendix 5- users amendment form (located electronically in the H Drive under ICT) to be completed as applicable when staff join and leave and a copy kept in the main school office

Employees of the school

Name		Website access	Email address	Frontline trip log on	SIMS log on	H drive access	AUP?	**Date of leaving**	**Date removed?**	Notes

Governors

Name	Website access	Email address	Frontline trip log on	AUP?	**Date of leaving**	**Date removed?**	Notes