Shenington Church of England Primary School
Stocking Lane, Shenington, Oxon OX15 6NF
Telephone 01295 670273
Email:office.5200@shenington.oxon.sch.uk

POLICY DOCUMENT

Excellence Through Endeavour
"Let your Light Shine" – Matthew 5:16

ICT Acceptable Use Policy

Introduction

ICT (Information and Communication Technology) is an essential resource to support learning and teaching, as well as playing an important role in the everyday lives of children, young people and adults. Consequently, as a school we ensure we have built in the use of these technologies in order to arm our young people with the skills to access life-long learning and employment. ICT covers a wide range of resources including web-based and mobile learning. It is also important to recognise the constant and fast-paced evolution of ICT within our society as a whole.

Whilst technology is exciting and beneficial both in and out of the context of education, many ICT, particularly web-based resources, are not consistently policed. All users need to be aware of the range of risks associated with the use of these internet technologies.

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

Schools hold personal data on learners, staff 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.

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 should be made aware of the risks and threats and how to minimise them.

Monitoring

Authorised ICT staff may inspect any ICT equipment owned or leased by the School at any time without prior notice. If a member of staff is in doubt as to whether the individual requesting such access is authorised to do so, please ask for their identification badge and contact the Head Teacher.

ICT authorised staff may monitor, intercept, access, inspect, record and disclose telephone calls, email, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving the school's 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 General Data Protection Regulation (GDPR); or to prevent or detect crime.

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

All monitoring, surveillance or investigative activities are conducted by ICT authorised staff and comply with the General Data Protection Regulation (GDPR), 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 equipment may be unavoidably included in any business communications that are monitored, intercepted and/or recorded.

Incident Reporting

Any security breaches, personal data breaches or attempts, loss of equipment and any unauthorised use or suspected misuse of ICT must be immediately reported to the ICT Coordinator or Head Teacher.

Incident Log

Some incidents may need to be recorded in other places, for example if they relate to a cyberbullying, up skirting or a racist incident. The designated Safeguarding Lead must be informed immediately.

Computer Viruses

- All files downloaded from the Internet, received via email or on removable media (e.g. CD, memory stick, external hard drives, memory cards) must be checked for any viruses using school provided antivirus software before using them. School staff must check with the ICT Coordinator before using any personal media storage devices.
- Staff must never interfere with any anti-virus software installed on school ICT equipment that they use.
- If anyone suspects that there may be a virus on any school ICT equipment, they should stop using the equipment and contact the ICT Coordinator/ ICT Support Provider immediately.
- School staff must not install any software or hardware equipment (including for example memory drives, data storage devices or computer programmes) without the permission of the ICT Coordinator.

Email

The use of email is an essential means of communication for both staff and pupils. In the context of school, email should not be considered private. Educationally, email can offer significant benefits including direct written contact between schools on different projects be they staff-based or pupil-based within school or international. We recognise that pupils need to understand how to style an email in relation to their age and good network etiquette 'netiquette'.

Managing Email

- The School gives all staff their own email account to use for all school business as a work-based tool. This is to minimise the risk of receiving unsolicited or malicious email 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 email histories can be traced. The school email account should be the account that is used for all school business.
- Under no circumstances should staff contact pupils, parents or conduct any school business using personal email addresses.
- The School requires a standard disclaimer to be attached to all email correspondence stating that; 'the views expressed are not necessarily those of the school or the Local Authority (LA)'. The responsibility for adding this disclaimer lies with the account holder.
- All email should be written and checked carefully before sending in the same way as a letter written on school headed paper.
- Pupils may only use school-approved accounts on the school system and only under direct teacher supervision for educational purposes.

- Email created or received as part of a position within the school will be subject to disclosure in response to a request for information under the Freedom of Information Act 2000. Staff must therefore actively manage their email account as follows. Delete all email of short-term value. Organise email into folders and carry out frequent house-keeping on all folders and archives.
- All pupil email users are expected to adhere to the generally accepted rules particularly in relation to the use of appropriate language, not revealing any personal details about themselves or others in email communication, not arranging to meet anyone without specific permission and also checking attachments for viruses.
- Pupils must immediately tell a teacher/ trusted adult if they receive an offensive email.
- Staff must inform the ICT Coordinator or Head Teacher if they receive an offensive email.
- Pupils are introduced to email as part of the Curriculum.
- All the school email policies apply however school email accounts are accessed (whether directly, through webmail when away from the office or on non-school hardware)

Sending Email

- Staff and pupils should only use their own school email account so that they can be clearly identified as the originator of a message.
- Senders should keep the number and relevance of email recipients, particularly those being copied, to the minimum necessary and appropriate.
- Senders should not send or forward attachments unnecessarily. Whenever possible, send the location path (hyperlink) to the shared drive rather than sending attachments.
- School email is not to be used for personal advertising.
- Staff are to check recipients carefully before sending, as this is a common cause of data breaches.

Receiving Email

- Email should be checked regularly.
- Attachments from an untrusted source should never be opened.
- Email systems should not be used to store attachments. Business-related work should be detached and saved to the appropriate shared drive/folder

Managing the School E-safety/Online Safety Messages

- We endeavour to embed e-safety/online safety messages across the curriculum whenever the internet and/or related technologies are used.
- The e-safety/online safety policy will be introduced to the pupils at the start of each school year.
- E-safety/online safety posters will be prominently displayed around school.

Cyberbullying

Cyberbullying is making use of information and communications technology, particularly mobile phones and the internet, to deliberately undermine, humiliate or otherwise cause distress to the person on the receiving end.

- Staff must not use social media and the internet to attack, insult, abuse or defame students, their family members, colleagues, other professionals, other organisations Shenington C of E VA Primary School.
- The person does not need to directly experience this form of victimisation in order for it to be classed as cyberbullying/harassment. The fact that a person is unaware that offensive or derogatory comments about them have been placed on websites still fits the criteria of cyberbullying/harassment.
- Staff should not personally engage with cyberbullying incidents and should immediately report incidents to the Head Teacher.
- If a member of Staff is the victim (receives any threats, abuse or harassment from members of the public through their use of social media), they should keep any records of the abuse and if appropriate, screen prints of messages or webpages with time, date and address of the site. Staff must report such incidents using the school's procedures.
- The school will consider it a potential disciplinary matter if users utilise any information and communications technology, including email and social networking sites, in such a way as to bully/harass others in the school or in partner organisations, or pupils or parents, whether this takes place during or outside of work.
- Staff members and pupils need to be aware that no matter what the privacy settings on their social media/networking site, inappropriate/derogatory information about a colleague in the school or partner organisations, other pupils or parents, can find its way into the public domain even when not intended.
- If a member of staff is the perpetrator of the incident(s) the situation will then be investigated and if appropriate, disciplinary action will be taken.
- If a pupil is the perpetrator of the incident(s) the situation will be initially investigated by the Head Teacher. Where appropriate the LA and/or police will be consulted.
- Where a potential criminal offence has been identified, and reported to the police, the School will ensure that any internal investigation does not interfere with police enquires.
- Staff who are victims of cyberbullying or harassment will be offered support by their line manager and where suitable, occupational health.
- Staff and victims are encouraged to preserve all evidence (e.g. by not deleting email, logging phone calls and taking screen-prints) which will help towards supporting an investigation. If the incident involves illegal content or contains threats of a physical or sexual nature, the Head Teacher should consider advising the employee that they should inform the police. In the event that such evidence contains indecent images of children, it is an offence to save, send, or alter an image or to show it to anyone else. Therefore, the evidence must be placed in a secure location such as a locked

cupboard where others will not be able to see it. In these circumstances the Police should be contacted immediately for advice.

Pupils with Additional Needs

The school endeavours to create a consistent message with parents for all pupils and this in turn should aid establishment and future development of the school's e-safety/online safety rules. However, staff are aware that some pupils may require additional teaching including reminders, prompts and further explanation to reinforce their existing knowledge and understanding of e-safety/online safety issues. Where a pupil has poor social understanding, careful consideration is given to group interactions when raising awareness of e-safety/online safety. Internet activities are planned and well managed for these children and young people.

Misuse and Infringements

Complaints

Complaints and/or issues relating to e-safety should be made to the Head Teacher. All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the ICT Coordinator or Head Teacher.

- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the ICT Coordinator and depending on the seriousness of the offence investigation by the Head Teacher/ LA and immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.
- Users are made aware of sanctions relating to the misuse or misconduct.

Internet Access

The internet is an open communication medium available to all at all times. Anyone can view information, send messages, discuss ideas and publish material which makes it both an invaluable resource for education, business and social interaction, as well as a potential risk to young and vulnerable people.

Managing the Internet

- The school students will only have supervised access to Internet resources through the school's internet technology.
- Staff will preview any recommended sites before use.
- Raw image searches are discouraged when working with pupils.
- If Internet research is set for homework, specific sites will be suggested that have previously been checked by the teacher. 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.

Internet Use

- Users must not post personal, sensitive, confidential or classified information or disseminate such information in any way that may compromise its intended restricted audience.
- Users must not reveal names of any member of our school community or any other confidential information acquired through the school on any social media platforms.
- Online gambling or gaming is not allowed.
- It is at the Head Teacher's discretion on what internet activities are permissible for staff and pupils and how this is disseminated.

Infrastructure

- School internet access is controlled through an external Proxy Server/web filtering service.
- Shenington School is aware of its responsibility when monitoring staff communication under current legislation and takes into account the General Data Protection Regulation (GDPR), the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, Regulation of Investigatory Powers Act 2000 and Human Rights Act 1998.
- Staff and pupils are aware that school-based email and internet activity can be monitored and explored further if required.
- The School does not allow pupils access to internet logs.
- The School uses management control tools for controlling and monitoring workstations.
- If staff or pupils discover an unsuitable site, the screen must be switched off/ closed and the incident reported immediately to the ICT Coordinator or Head Teacher as appropriate.
- It is the responsibility of the school, by delegation to the ICT Support Provider, 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 ICT Support Provider's to install or maintain virus protection on personal systems. If pupils wish to bring in work on removable media, they must be given to the teacher for a safety check first.
- Pupils and staff are not permitted to download programs or files on school based technologies without seeking prior permission from the Head Teacher or ICT Coordinator.

- If there are any issues related to viruses or anti-virus software the ICT Support Provider should be informed.

Use of Social Media

- Please see Social Media Policy

Children's ICT Rules

Children are asked to sign an ICT Acceptable Use Agreement and adhere to the ICT Rules which have been designed to safeguard them when they are online. Children are also asked to take good care of the School's ICT equipment. Any misuse or deliberate damage to school equipment will not be tolerated. Parents may be asked to contribute to any costs involved in repairing/replacing equipment damaged by their child.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting e-safety/online safety both in and outside school and also to be aware of their responsibilities. We regularly consult and discuss e-safety/online safety with parents/ carers and seek to promote a wide understanding of the benefits related to ICT and associated risks.

- Parents/ carers and pupils are actively encouraged to contribute to adjustments or reviews of the school e-safety/online safety policy.
- Parents/ carers are asked to read through and sign an Acceptable Use Agreement on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they consent to images of their child being taken/ used in the public domain (e.g. on school website).
- The school disseminates information to parents relating to e-safety/online safety, where appropriate, in the form of:
    - Information and celebration evenings
    - Posters
    - Website postings
    - Newsletter items
    - E-safety/online safety talks

Safe Use of Images

Taking of Images and Film

Digital images are easy to capture, reproduce and publish and, therefore, misuse. We must remember that it is not always appropriate to take or store images of any member of the school community or public without first seeking consent and considering the appropriateness.

- With the written consent of parents (on behalf of pupils) and staff, the school permits the appropriate taking of images by staff and pupils with school equipment.

- Staff and representatives acting on behalf of the school are not permitted to use personal digital equipment, such as mobile phones, to record images of pupils, this includes when on field trips. However, with the express permission of the Head Teacher, images can be taken provided they are transferred immediately and solely to the school's network and deleted from the staff device.
- All personnel working with children on-site will have their personal mobile phones/device silenced and left in the staff room or school office. Should anyone need to use their personal phone/device, this will be done in the staff room, school office or in front of the building and not in the vicinity of children.
- All visitors will have their personal mobile phones/device silenced and left in the school office. Should any visitors need to use their personal phone/device, this will be done in the school office or in front of the building and not in the vicinity of children.

Publishing Pupil's Images/Videos and Work

On a child's entry to the school, all parents/carers will be asked to give permission to use their child's work or image/video in the following ways:

- On the school website.
- In the school prospectus and other printed publications that the school may produce for promotional purposes.
- In display material that may be used in the school's communal areas.

The School will ask you first if we wish to use your child's photo for any other reason, for example:

- In display material that may be used in external areas e.g. 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).

This consent form is considered valid for the entire period that the child attends this school unless there is a change in the child's circumstances where consent could be an issue, e.g. divorce of parents, custody issues, etc. Parents/ carers may withdraw permission, in writing, at any time. Consent has to be given by both parents in order for it to be deemed valid. Pupils' names will not be published alongside their images and vice versa. Email and postal addresses of pupils will not be published. Pupils' full names will not be published.

Conditions of use of Pupil's Images/Videos

Conditions of use of Pupil's Images/Videos include:

- We will not re-use any images or video recordings after your child leaves the school.
- We will not include the personal details or full names of any child with an image or in any of our printed publications, web pages or videos (if there is the intention to use a full name of a pupil, the school will seek permission separately on each occasion).

- We will not include personal email or postal addresses, or telephone numbers in any of our printed publications, websites or video recordings.
- If we use images of individual or small groups of pupils, we will include the name of that child and the first letter of their surname in any accompanying text or image caption without good reason. If we name a pupil in the text, we will not use an image of that child to accompany the article without good reason e.g. the inclusion of the full name and image of a competition winner.
- We may include pictures of pupils that have been drawn by pupils.
- We may use group or class images or video recordings with very general captions only such as ‘making Easter decorations’.
- We will only use images of pupils who are suitably dressed to reduce the risk of any inappropriate use.

Storage of Images

- Images/ films of children are stored on the school’s network initially and the transferred to digital storage media (e.g. CD, external hard drive) which are then stored in a locked cupboard in the office area.
- Pupils and staff are not permitted to use personal portable media for storage of images (e.g. memory sticks) without the express permission of the Head Teacher.
- Rights of access to this material are restricted to the teaching staff and pupils within the confines of the school network.

Webcams and CCTV

- Webcams in school are only ever used for specific learning purposes
- Misuse of the webcam by any member of the school community will result in disciplinary action.

Upskirting

Any incidents of upskirting (the act of secretly taking a photo or filming under an individual's clothing without their permission) must be reported to the Designated Safeguarding Lead. Where appropriate the LA and/or police will be consulted.

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

School ICT Equipment

- Any users of ICT are responsible for any activity undertaken on the school's ICT equipment provided to them.
- The school keeps a log of ICT equipment issued to staff and records serial numbers as part of the school's inventory.
- Visitors are not allowed to plug their ICT hardware into the school network points (unless special permission has been given by the ICT Coordinator or Head Teacher.
- All ICT equipment should be kept physically secure.
- Staff must not attempt unauthorised access or make unauthorised modifications to computer equipment and programs. They can modify or delete their own files or data, but other system files and data should not be accessed or altered. This is an offence under the Computer Misuse Act 1990.
- It is imperative that all data are saved on a frequent basis to the school's network drive. Staff are responsible for the backup and restoration of any data that are not held on the school's network drive.
- Personal or sensitive data should not be stored on the local drives of desktop computers or laptops. If it is necessary to do so the local drive must be encrypted.
- It is recommended that a timed screensaver is applied to all machines.
- Any devices accessing personal data must have a timed screensaver as must any user profiles which requires a password on return.
- Privately-owned ICT equipment should not be used in school or on a school network unless special permission has been given by the senior leadership team or ICT Support Provider.
- On termination of employment, all ICT equipment must be returned to the Head Teacher. Staff must also provide details of all their system logons so that they can be disabled.
- It is the responsibility of every member of staff to ensure that any information accessed from their own PC or removable media equipment is kept secure, and that no personal, sensitive, confidential or classified information is disclosed to any unauthorised person.
- All redundant ICT equipment is disposed of in accordance with Waste Electrical and Electronic Equipment (WEEE) directive and Data Protection Act (DPA)

Portable & Mobile ICT Equipment

- This section covers such items as laptops, tablets and removable data storage devices.
- All activities carried out on School systems and hardware will be monitored in accordance with the general policy.
- Staff must ensure that all school data are stored on school's network, and not kept solely on the laptop. Any equipment where personal data are 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 laptops will be placed in the boot of the car before starting the journey and will not be left in the car if it is unattended.
- All locally stored data, including diary entries, must be synchronized with the central school network server on a frequent basis.
- Portable and mobile ICT equipment must be made available as necessary for antivirus updates and software installations, patches or upgrades.
- The installation of any applications or software packages must be authorised by the ICT Coordinator, fully licensed and only carried out by the school's ICT Support Provider.
- In areas where there are likely to be members of the general public, portable or mobile ICT equipment must not be left unattended and, wherever possible, must be kept out of sight.
- Portable equipment must be transported in its protective case if supplied.

Emerging Technologies

Many emerging technologies offer new opportunities for teaching and learning including a move towards personalised learning and 1:1 device ownership for children and young people. Many existing mobile technologies such as tablets, portable media players, gaming devices, mobiles and smart phones are familiar to children outside of school too. They often provide a collaborative platform with possible internet access and thus open up risk and misuse associated with communication and internet use. Emerging technologies will be examined for educational benefit and the risk assessed before use in school is allowed.

AI (Artificial Intelligence)

The school recognises that Artificial Intelligence (AI), including generative AI tools, presents both opportunities and risks within an educational setting.
The use of AI within the school will be carefully controlled and monitored to ensure compliance with data protection law, safeguarding responsibilities, and other legal and ethical obligations.

Risks
The school acknowledges risks associated with the use of AI, including:

- Unauthorised disclosure of personal or sensitive data
- Inaccurate or biased outputs leading to unfair treatment
- Copyright and intellectual property concerns
- Safeguarding risks
- Lack of transparency in AI-generated decisions

Use of AI

- Pupils must not use AI tools unless explicitly authorised and supervised by the school.
- Where AI tools have age restrictions, these must be adhered to.
- Staff must not input personal data, special category data, or confidential school information into AI tools unless the tool has been formally approved by the school and appropriate safeguards are in place.
- Any proposed use of AI must be reviewed and approved by the Headteacher (or delegated senior leader) to ensure it is appropriate, lawful, and proportionate.

Data Protection

- All use of AI must comply with UK GDPR and the Data Protection Act 2018.
- Personal data must only be processed where there is a clear lawful basis.
- Data minimisation must be applied at all times.

Governance and Reporting

- Staff and governors must raise any concerns about the use or proposed use of AI with the Headteacher in the first instance.
- Any data protection breaches involving AI must be reported in line with the school's data breach procedures.
- Any safeguarding concerns arising from the use of AI must be reported immediately to the Designated Safeguarding Lead (DSL) in accordance with the school's safeguarding policy.

Monitoring and Review

- The school will keep the use of AI under review and update this policy as technology and guidance evolves.

E-safety and Cyberbullying Toolkit

The Oxfordshire County Council E-safety and Cyberbullying Toolkit (April 2019) provides information and resources for promoting e-safety/online safety of children and young people and preventing and tackling cyberbullying.

http://schools.oxfordshire.gov.uk/cms/sites/schools/files/folders/folders/documents/antibullying/policies/cyberbullyingtoolkit.pdf

Current Legislation

Acts Relating to Monitoring of Staff Communications

General Data Protection Regulation (GDPR)
The regulation requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The regulation grants individuals rights of access to their personal data, compensation and prevention of processing.

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/Online Safety

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 have a copy of "Children & Families: Safer from Sexual Crime" document as part of their child safeguarding processes.

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 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 persons 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 (email) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 1988
Copyright is the right to prevent others from copying or using work without permission. Works such as text, music, sound, film and programs all qualify for copyright protection. The author of the work is usually the copyright owner, but if it was created during the course of employment it belongs to the employer. Copyright infringement is to copy all or a substantial part of anyone's work without obtaining them author's permission. Usually a licence associated with the work will allow a user to copy or use it for limited purposes. It is advisable always to read the terms of a licence before you copy or use someone else's

material. It is also illegal to adapt or use software without a licence or in ways prohibited by the terms of the 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 1978 (Section 1)
It is an offence to take, permit to be taken, make, possess, show, distribute or advertise indecent images of children in the United Kingdom. A child for these purposes is anyone under the age of 18. Viewing an indecent image of a child on your computer means that you have made a digital image. An image of a child also covers pseudo-photographs (digitally collated or otherwise). A person convicted of such an offence may face up to 10 years in prison.

Obscene Publications Act 1959 and 1964
Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Protection from Harassment Act 1997
A person must not pursue a course of conduct, which amounts to harassment of another, and which he knows or ought to know amounts to harassment of the other.

A person whose course of conduct causes another to fear, on at least two occasions, that violence will be used against him is guilty of an offence if he knows or ought to know that his 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 (GDPR)

The Freedom of Information Act 2000

Policy approved by:	**The Full Governing Body**
Policy adopted:	**June 2026**
Policy review date:	**June 2029**