E-SAFETY POLICY
September 2022 onwards

Related Policies and Documents:

- IT Usage Policy
- Safeguarding / Child Protection Policy
- Data Protection Privacy Notice
- Taking, Storing and Using Images of Children Policy

eSafety

The use of IT in the classroom inherently brings with it risks and concerns. As technology can be rapidly-evolving and also bring new and potentially unwanted capabilities, its use must be regularly reviewed and such risks addressed. Although not every risk requires a technical solution, both staff and pupils should be aware of the capabilities of the new technologies and, where there may be a potential issue, be made aware of how to assess and minimise the risks, bring issues to others' attention, and manage the issues raised. Such issues may not be limited to the classroom, and pupils should be made aware of eSafety risks that might present themselves in their daily lives too.

A few examples of the technologies in use today that may bring associated risks are:

- Email
- Chat-rooms and social networking services
- Mobile phones and smartphones
- Tablet Apps which store or share information
- Cloud computing services, such as Google Drive

However this is by no means an exhaustive list and new technologies are liable to emerge, bringing new risks, all the time.

The School has a responsibility to educate pupils and staff on eSafety issues associated with these, and any other, technologies to allow both to learn how to safely use them and deal with problems that arise.

The School's associated policies, including the IT Usage Policy, should be designed to ensure the safety of all users, including teaching staff, administrative staff, governors, visitors and all pupils. Such policies should also pay heed to the management of data, much of which could potentially be misused to cause harm or distress to an individual if inadvertently disclosed. Policies should be designed with applicability to a range of modern technologies and revised as and when new types of threats are discovered.

Roles and Responsibilities

As eSafety is an important aspect of strategic leadership within the school, the Head, and Governors have ultimate responsibility to ensure that the policy and practices are embedded and monitored. The DSL takes lead responsibility for the online safety of the pupils. The Assistant Head - Digital Learning is the eSafety Coordinator and chairs the School's IT Development Committee, briefing the Head and Senior Leadership team on at least a termly basis. All members of the school have been made aware of who holds this post. It is the role of the eSafety Coordinator to keep abreast of current issues and guidance through external organisations such as Herts LA, DfE, CEOP (Child Exploitation and Online Protection) and Childnet and advise the DSL appropriately to develop appropriate resources to promote eSafety.

Senior Managers and Governors are updated by the Head / DSL / eSafety Coordinator 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 Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct is to protect the interests and safety of the whole school community.

eSafety skills development for staff and parents

As eSafety is not only a consideration in itself, but also an important part of the taught curriculum, teaching staff should receive regular information and training on eSafety issues in the form of Staff INSET Training. New staff receive information on the school's acceptable use policy as part of their induction.

All staff should be made aware of individual responsibilities relating to the safeguarding of children within the context of eSafety and know what to do in the event of misuse of technology by any member of the School.

Staff are made aware of eSafety information via their regular INSET training covering best practice and latest developments within this area. eSafety training is delivered by the School's Assistant Head - Digital Learning during these INSETs. The Assistant Head - Digital Learning will also communicate at any time during the academic year any matters of immediate concern to all staff and parents. External trainers may be invited to cover specific points during the year.

Parents should also be kept abreast of best practice in eSafety and made aware of eSafety information by coverage of the topic and the issuing of various eSafety materials at welcome meetings at the beginning of each school year. The school also hosts parent-specific eSafety information via the School's Intranet and weekly information and newsletters.

All groups sign an Acceptable Usage Policy which contains the essence of eSafety material, and are referred to further eSafety information. Pupils, parents and staff all have their own sections of eSafety reference material available through the School's Intranet system, including links to eSafety concern-reporting services.

eSafety in the Curriculum

As IT and online resources are increasingly used across the curriculum, it is essential for eSafety guidance to be given to pupils and staff on a regular and meaningful basis. The School should endeavour to embed eSafety messages across the curriculum whenever the Internet and / or related technologies are used.

- The school has a framework for teaching internet skills in IT and PSHE lessons as found in the Scheme of Work.
- The school should provide opportunities within a range of curriculum areas to include teaching of eSafety.
- Pupils should be taught about copyright and respecting other people's information, images, etc through discussion, modelling and activities.
- Pupils should be made aware of the impact of online bullying and know how to seek help if they are affected by these issues. Pupils should also be 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 Childline / CEOP.
- Pupils should be taught to critically evaluate materials and learn good search skills through cross curricular teacher models, discussions and via the IT curriculum.
- Pupils are made aware of eSafety information throughout the course of their studies in their IT lessons, included in the unit plans, as well as a specific emphasis at the start of the year and during issue of devices (e.g.Chromebooks).

Monitoring

It is a necessary requirement, given the responsibilities associated with the maintenance and monitoring of the IT equipment and policies, that authorised IT staff may need to inspect any IT equipment or data owned or controlled by the school at any time without prior notice.

Authorised IT staff may need to monitor, intercept, access, inspect, record and disclose telephone calls, emails, instant messaging, internet/intranet use and any other electronic communications (data, voice or image) involving its employees or contractors, without prior 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, as may be amended under GDPR, or to prevent or detect crime.

Pupil digital communications and files are monitored by a software system for safeguarding concerns under the categories of abuse, adult content, bullying, criminal activity, radicalisation, substance abuse and suicide. The Assistant Head - Digital Learning or IT Manager will review reports from the system, alerting the DSL of any safeguarding issues that arise.

All monitoring, surveillance or investigative activities are conducted by IT authorised staff and comply with the relevant legislations (see Appendix).

Please note that personal communications made using School IT equipment may be unavoidably included in any business communications that are monitored, intercepted and/or recorded. In accordance with the IT Usage Policy, however, use of the School Network should be for business purposes only.

Infrastructure

- Monitoring of web based activity is recorded and filtered by a proxy server, and other appropriate systems.
- The School is aware of its responsibility when monitoring staff communication under current legislation (see Appendix)
- Staff and pupils are aware that school-based email and internet activity - whether it is marked personal or otherwise - can be monitored and logged and can be made available on request to the Head or Bursar.
- The school does not allow users access to internet logs, except relevant portions as necessary to perform their job or investigate a reported incident.
- The school uses management control tools for controlling and monitoring workstations.
- If pupils discover an unsuitable website or usage of data, this should be reported immediately to their teacher.
- If staff discover an unsuitable website or usage of data, this should be reported immediately to the eSafety Coordinator and / or IT Manager.
- The network is monitored for unauthorised devices (e.g. USB sticks, mobile phones, Wifi points, etc.) to prevent data being stored on unmanaged or personal devices.
- Staff have been made aware of the additional requirements when working at home, via the school's Staff, Governor and Visitor Acceptable Use Agreement / Code of Conduct

Incident Reporting

A Data Breach Procedure has been issued to all staff to take account of the requirements under GDPR (General Data Protection Regulation).

Any:

- breaches of IT security, whether physical or data, or attempts to do so
- loss or suspected loss of equipment or data (including logon Credentials and security tokens)
- suspected inappropriate use of systems or data
- potential for, or actual revelation, of data to unauthorised persons
- unauthorised use or suspected misuse of IT
- contact between a pupil and an unauthorised person via the Internet
- concern regarding a pupil's or member of staff's use of the system

must be immediately reported to the school's Data Protection Manager, IT Manager, eSafety Coordinator or Designated Safeguarding Lead as appropriate.

In the event that illegal activity is detected or reported, the Senior Leadership Team and police should be informed and evidence preserved. If necessary, any access to the accounts or data involved that could be used to modify the evidence should be disabled or rescinded in order to preserve the evidence. In the event of police involvement, evidence should only be preserved, it should not be disseminated further.

If the activity involves children, or Child Protection, the School's Child Protection designated persons must be informed immediately.

All users of IT equipment or data (whether employees, contractors or pupils) are aware that a breach or suspected breach of policy may result in the temporary or permanent withdrawal of their access to school IT hardware, software or services. Any policy breach may also be grounds for disciplinary action in accordance with the school Disciplinary Procedure.

Password Security

Password security is essential for all users, but particularly staff as they are able to access and use pupil data. Staff are expected to have secure passwords to protect any data, or access to data, which they hold, and these details should not be shared with others except as absolutely necessary. Pupils are expected to keep their passwords secret and not to share with others, particularly their friends. Staff and pupils should be regularly reminded of the need for password security.

- All users (staff, visitors and pupils) read and sign an Acceptable Use Agreement to demonstrate that they have understood the School's eSafety and IT policies.
- Users are provided with an individual network login and (optionally) email username. From Year 3 they are also expected to use a personal password and keep it private.
- Pupils are not allowed to deliberately access data on the school network which belongs to someone else, whether pupil, teacher or other staff.
- If staff or pupils think their password may have been compromised or someone else has become aware of their password they know to report this to the Head of IT or IT Manager.
- Staff are aware of their individual responsibilities to protect the security and confidentiality of school networks and MIS, including ensuring that passwords are not shared and are changed periodically. Individual staff users must also make sure that logged-in workstations are not left unattended and are properly locked when they leave them.

Data Security

The accessing and appropriate use of school data is something that the school takes very seriously.

- Staff are aware of their responsibility when accessing school data.
- The level of access allowed by a given user is determined by the IT Manager in conjunction with the Senior Management Team, to be the minimum access necessary to perform the necessary elements of their job.

- Staff are aware that confidential pupil data should be treated as such and kept secure whether on or off the school premises.
- A Data Breach Procedure has been issued to all staff to take account of the requirements under GDPR (General Data Protection Regulation). This includes attempting to circumvent system security or to gain access to data beyond that which has been permitted.

Internet

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.

All use of the Internet at Edge Grove is logged and the logs are regularly monitored, both automatically and manually. Whenever any inappropriate use is detected it will be followed up.

- The school maintains that all students will have supervised access to Internet resources (where reasonable) through the school systems.
- The use of the Internet through school devices should be in support of education and research and be consistent with the educational objectives of Edge Grove.
- No child may have access to a school device capable of connecting to the Internet without adult supervision.
- Staff must actively monitor every workstation in the room to obviate any possibility of misdemeanour or inappropriate use. Staff have access to monitoring software for this purpose.
- Use of other organisations' network or computing resources must comply with the rules appropriate for that network.
- Staff should preview any recommended websites or other resources before use to ensure suitability.
- Raw, or on-the-fly, images and other searches are to be discouraged when working with pupils.
- If Internet research is set for work outside of school (Prep work, extension work, etc.), specific websites or resources will be suggested that have previously been checked by the teacher. It is advised that parents check these resources and supervise this work.
- All users must observe software, image and other works' copyright at all times.

Social Networking and "Wiki" sites

Social networking sites, forums and editable-content sites (e.g. "Wiki" sites such as Wikipedia), if used responsibly both outside and within an educational context, can provide easy to use, creative, collaborative and free facilities. However it is important to recognise that there are issues regarding the appropriateness of some content or contact. To this end, the School encourages all pupils to think carefully about the way that information can be added and removed by all users, including themselves, from these sites.

At present, the School endeavours to deny access to social networking sites to pupils within school, however we recognise that pupils may have access to these social networking sites from home and we will advise them of the risks in IT and PSHE lessons at school.

Staff use of such sites should be approved by the Head of IT and the Head, and be limited to use on an educational basis.

To this effect:

- All pupils are advised to be cautious about the information given by others on sites, for example users not being who they say they are.
- Pupils are always reminded to avoid giving out personal details on such sites which may identify them or where they are (full name, address, mobile/ home phone numbers, school details, IM/ email address, specific hobbies/ interests, etc.).
- Pupils are taught to avoid placing images of themselves (or details within images that could give background details) on such sites and to consider the appropriateness of any images they post.
- Pupils are advised that once information has been transmitted on the Internet, it is usually extremely difficult, if not impossible, to rescind. Particular examples include sites which may claim to "delete" posted images after a few minutes, or archive sites which may still hold copies of data posted accidentally. Because of the possibility of records of that data being collected by others (including screenshots of posted images, or permanent copies of data posted only fleetingly), pupils are advised to always treat data placed onto the Internet as permanent, no matter the guarantees given by the site in question.
- 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 via any medium to the school, wherever and whenever they may occur.

Email

The use of email within School is an essential means of communication for both staff and pupils and, as such, merits explicit mention.

The school gives all staff their own email account to use for all school business. This is to protect staff, minimise the risk of receiving unsolicited or malicious emails, allow monitoring and avoids the risk of personal information being revealed. Staff are aware that all school business email should be conducted by their school email account and not their personal accounts.

Some groups of pupils are also given their own email account to use for school business. Pupils may only use school approved accounts on the school system and only under direct teacher supervision for necessary purposes.

It is the responsibility of each user to keep the account password secure and to exercise care in where they reveal their email address. Pupils should not reveal personal information in email, nor should they disseminate their email address to others that they do not know. For the safety and security of users and recipients, all school email is filtered and logged; if necessary email histories can be traced.

Email can be sent by services provided by the school (e.g. Google) and is also able to be sent via a number of in-school services, such as ClarionCall, SchoolBase, Scan-to-Email or other automated tools. Whichever method is used to send mail, from whatever device, the same principles and policies apply.

In all communication, the number and relevance of email recipients, particularly those being copied, should be kept to the minimum necessary and appropriate. Personal data should not be sent via email. Where necessary, data must be sent via an encrypted medium, such as an encrypted memory card, secure web service, etc.

Email sent from the main account on the school system must include a standard disclaimer, stating that, 'the views expressed are not necessarily those of the school'. Email to pupils which is inappropriate, or may cause distress or anxiety, must be reported to a member of staff. Similarly, staff

must inform their line manager if they receive an offensive or inappropriate email. Examples of this include messages containing offensive terms or abuse, “chain letters”, actions or statements that may be perceived as bullying, etc.

Mobile technologies

As with any new trend, the use of mobile technologies should take account of their capabilities and their place within the existing policy framework. Notably, appropriate measures should be taken to control and monitor mobile devices which are supplied or authorised by the school.

Purchasing of individual devices (such as tablet or mobile computers) should take account of the device’s capabilities, for example if they are able to directly connect to the Internet thereby bypassing filtering and other measures. Where possible, such devices should be monitored and controlled by the existing systems in place so as to provide the fewest avenues that require securing and, as a general rule, are never issued to pupils.

The School manages authorised mobile devices through the use of Mobile Device Management. Tablet and mobile computers are restricted to wireless use only and, thus, are monitored and controlled by the existing network infrastructure. The systems allow, through the use of enforced settings, management software and “talk-home” technology, both blocking and erasure of lost devices to prevent unauthorised access to data. Mobile devices that might contain personal data (e.g. staff tablets or mobile computers) are PIN-protected to prevent access to the data in the case of loss of the device. Laptops and other devices taken off-site that may contain personal data are encrypted, and passwords stored separately.

Staff personal mobile telephones are permitted on-site (specific additional rules apply in the EYFS) but should not be used in the classroom or for school business purposes and must not compromise the safety of pupils or their data. It is not permitted to use them to bypass security measures on the network (e.g. to access a filtered website) or to take or store photographs other than in accordance with the Policy on Taking, Storage and Using Images of Children.

The school is not responsible for the loss, damage or theft of any personal device. Users bringing personal devices into school must ensure there is no inappropriate or illegal content on the device, and are responsible for any such content. Users are also responsible for any interference or disruption that their personal device may cause.

In all cases, on school devices or personal, permission must be sought before any image or sound recordings are made on these devices of any member of the school, in relation to the Policy on Taking Storing and Using Images of Children and other relevant policies. The sending of inappropriate text messages, or the communication of any inappropriate voice messages, by any member of the School is not allowed.

Where devices are provided by the school, such devices are to be used for school purposes only.

Photography and images

As digital images have become easier to produce and disseminate, it is necessary to control their use to prevent inadvertent, or undesirable, distribution.

The School has a *Policy on Taking, Storage and Using Images of Children*, which controls the use and taking of such images. Given the activities taking place within the school, school-sanctioned photography of children is generally permitted for purposes of internal identification (e.g. pupil ID photos on the school system), promotion, displays, etc although these should be taken on a school owned camera whenever possible. Permission must be obtained from parents in the case where photos of children are to be used in promotional materials or other publications. Staff should not use personal cameras or smart phones without permission of the Senior Management Team.

Care is taken to ensure that pupils in photographs displayed publicly cannot be identified or linked to personal details such as their name, etc. Parents are permitted to take photographs under certain conditions, as detailed in the *Policy on Taking, Storage and Using Images of Children*.

Pupils with Additional Needs

The school endeavours to create a consistent message for all pupils and this in turn should aid establishment and future development of the school's eSafety rules.

However, staff are aware that some pupils may require additional support or teaching including adapted resources, reminders, prompts and further explanation to reinforce their existing knowledge and understanding of eSafety issues.

Parental Involvement

We believe that it is essential for parents/ carers to be fully involved with promoting eSafety both in and outside of school.

- Parents/ carers are asked to read through and sign acceptable use agreements on behalf of their child on admission to school.
- Parents/ carers are required to make a decision as to whether they object to images of their child being taken/ used in the public domain (e.g., on school website). Instructions as to the correct procedure to register an objection are contained in the School's Terms & Conditions.
- Parents are also invited to eSafety briefings aimed at protecting their children from the risks involved with electronic communication, both at home and the measures deployed in-school.

Misuse, Infringements and Complaints

Any misuse of devices, or infringement of the eSafety policies of the school, may incur disciplinary actions. Complaints relating to eSafety should be made to the eSafety Coordinator, Senior Deputy Head or Head. All such complaints should be logged and appropriately responded to.

Inappropriate material

- All users are aware of the procedures for reporting accidental access to inappropriate materials. The breach must be immediately reported to the eSafety Coordinator.
- Deliberate access to inappropriate materials by any user will lead to the incident being logged by the eSafety Coordinator, depending on the seriousness of the offence; investigation by the Head, immediate suspension, possibly leading to dismissal and involvement of police for very serious offences.

Policy Review

Given the fast-paced movement of technology, the eSafety policy, more than most others, should be reviewed regularly for inaccuracies or missing clarifications. There is an ongoing opportunity for staff to discuss with the eSafety Coordinator any issue of eSafety that concerns them.

This policy will be reviewed at least annually and consideration given to the implications for future whole school development planning. The policy should be amended if new technologies are adopted or new eSafety concerns arise, if such concerns are not already addressed by the existing policy.

This policy was last revised:

Date	Person	Position
September 2022	Ian Kay	Assistant Head - Digital Learning

At date of Revision, the following post holders were applicable to this policy:

eSafety Co-ordinator:	Ian Kay – Assistant Head - Digital Learning
IT Manager:	Lee Dowling
Designated Safeguarding Lead:	Jo Leighton – Senior Deputy Head
Data Protection Manager	Gillian Dippenaar

EDGE GROVE

Acceptable Use Agreement / eSafety Rules
(Years 3, 4, 5, 6)

- I will only use IT in school for school purposes.
- I will only use my class email address or my own school email address when emailing.
- I will only open email attachments from people I know, or who my teacher has approved.
- I will not tell other people my IT passwords.
- I will only open/delete my own files.
- I will make sure that all IT contact with other children and adults is responsible, polite and sensible.
- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I will not give out my own details such as my name, phone number or home address. I will not arrange to meet someone unless this is part of a school project approved by my teacher and a responsible adult comes with me.
- I will be responsible for my behaviour when using IT because I know that these rules are to keep me safe.
- I know that my use of IT can be checked and that my parents / carer can be contacted if a member of school staff is concerned about my eSafety.

Dear Parent / Carer,

IT, including the Internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all children to be safe and responsible when using any IT.

Please read and discuss these eSafety rules with your child and return the slip at the bottom of this page. If you have any concerns or would like some explanation please contact the School eSafety Coordinator.

Parent / Carer signature
We have discussed this and …….....(child name) agrees to follow the eSafety rules and to support the safe use of IT at Edge Grove School.

Parent Signature ……

Form ……. Date ……

EDGE GROVE

Acceptable Use Agreement / eSafety Rules
(Years 7 & 8)

- I will only use IT systems in school, including the internet, email, digital video, mobile technologies, etc, for school purposes.
- I will not download or install software on school systems or devices.
- I will only log on to the school systems with my own username and password.
- I will follow the school's IT security system and not reveal my passwords to anyone.
- I will only use my school email address.
- I will make sure that all communication with pupils, teachers or others is responsible and sensible. I will ensure that my online activity, both in school and outside school, will not cause my school, the staff, pupils or others distress or bring the school into disrepute.
- I will be responsible for my behaviour when using the Internet. This includes resources I access and the language I use.
- I will not deliberately browse, download, upload or forward material that could be considered offensive or illegal. If I accidentally come across any such material I will report it immediately to my teacher.
- I will not give out any personal information such as my name, phone number or address. I will not arrange to meet someone unless this is part of a school project approved by my teacher.
- I will not take images of pupils and/ or staff except for school purposes, and in line with school policy, and will not distribute these outside the school without the permission of a teacher.
- I will respect the privacy and ownership of others' work online at all times.
- I will not attempt to bypass the School's internet filtering system, or other security measures.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available to my teachers.
- I understand that these rules are designed to keep me safe and that if they are not followed, school sanctions will be applied and my parents/ carer may be contacted.

Dear Parent / Carer,

IT, including the internet, email and mobile technologies, etc. has become an important part of learning in our school. We expect all pupils to be safe and responsible when using any IT. It is essential that pupils are aware of eSafety and know how to stay safe when using any IT.

Pupils are expected to read and discuss this agreement with their parents or carer and then to sign and follow the terms of the agreement. Any concerns or explanation can be discussed with their class teacher or the School eSafety Coordinator.

Please return the bottom section of this form to school for filing.

Pupil and Parent / Carer signature

We have discussed this document and …….....(pupil name) agrees to

follow the eSafety rules and to support the safe and responsible use of IT at Edge Grove School.

Parent Signature …….

Pupil Signature ……

Form ……. Date ……

Appendix 1: Relevant Legislation

Acts relating to monitoring of staff email

- Data Protection Act 1998 (http://www.hmso.gov.uk/acts/acts1998/19980029.htm)
  The Act requires anyone who handles personal information to comply with important data protection principles when treating personal data relating to any living individual. The Act grants 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)

  and

- Regulation of Investigatory Powers Act 2000
  (http://www.hmso.gov.uk/acts/acts2000/20000023.htm)
  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.

- Human Rights Act 1998 (http://www.hmso.gov.uk/acts/acts1998/19980042.htm)

Other Acts relating to eSafety

- Racial and Religious Hatred Act 2006
  It is 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
  A grooming offence can be committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) with the intention to commit certain sexual offences. It is an offence to meet them or travel to meet them anywhere in the world with such intentions. 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.

- 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 (for example, attacks on servers, or changings of settings with such intention).

- Malicious Communications Act 1988 (section 1)
  This legislation makes it a criminal offence to send an electronic message 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. Copyright infringement is 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 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 incite 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 (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).

- 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.