Acceptable use of IT Policy

(including cameras)

Acceptable Use of IT Policy (Including EYFS)

Policy Review Date: Sept 2022
Reviewed By: M Ashton & SLT
Next Review: Sept 2023 (or following incident, legislation or interim guidance)

Distribution

Please note that 2 copies of this policy are printed as standard and distributed to the following areas:

1) Staff Room
2) School Office

This policy is also made available on the school website.

Updates and Amendments to Policy

Date	Section Heading	Update Details	Page N°
28/01/2019	2.1 Internet and Email	The teacher must report it to the Computing Coordinator who must complete an incident section in the 'Online Safety Log' and follow the procedures as set out in the 'E-Safety Policy'.	5
28/01/2019	2.1 Internet and Email	THE DATA PROTECTION ACT (1998) and THE GENERAL DATA PROTECTION REGULATION (GDPR)(2018)	6
28/01/2019	2.4 PHOTOGRAPHS AND IMAGES	Webcams may be used to Skype as planned by the teacher and agreed by the SLT. Prior Parental consent must be obtained for any other broadcast on the internet.	9
28/01/2019	APPENDIX 2 - RELATED LEGISLATION	Data Protection Act 2018 (incorporating GDPR) https://www.gov.uk/government/collections/data-protection-act-2018	14 and 17
01/03/2020	1.1 Introduction	Online cloud based Environments such as Mathletics, Oxford Reading Buddy.	5
01/03/2020	1.2 Aims	Within the context of our safeguarding policy. See also our PSHEE policy.	6
01/03/2020	Cyber-bullying	Texting scary or rude messages by electronic devices. Sending unpleasant photographs by electronic devices. (includes definition and advice on 'upskirting')	7
01/03/2020	The Data Protection Act	Where staff are using EY log (or similar system) to track and provide information for parents on their child's progress, the software is stored on school-owned devises and can be used by EYFS authorised personnel only.	8
01/03/2020	Use of children's names in email	Avalon School have secure drives where any sensitive or confidential information about a pupil	8

		can be stored and only those staff who have need to know are able to see it.	
01/03/2020	2.2 Access and security	All staff and KS2 children have their own logons to the school network. Access to secure drives on the network are given to those staff who have permission as agreed with the SLT. No one should let anyone else know their passwords. Any sensitive information (eg school reports) held on portable storage devices such as memory sticks, must be password protected. If the SLT have reasonable cause to think that a member of staff's device has been used in contravention of this policy or other school policies then the SLT may insist that the device be examined in an unlocked state and if using the school network, their logon folders will be viewed. (For example, inappropriate pictures taken of pupils). Where staff are using EY log (or similar system) to track and provide information for parents on their child's progress, the software is stored on school-owned devises and can be used by EYFS authorised personnel only.	9
01/03/2020	2.3 Mobile electronic devices protocol	Mobile electronic device now includes 'wearable technology'.	10
Jan 2021	Updated after review	Highlighted in green	
September 2022	Updated after review		

CONTENTS

1. RATIONALE

1.1 INTRODUCTION

At Avalon School we strive to deliver our curriculum in a safe, caring and positive environment.

Avalon School seeks to make sure that all staff, pupils and parents are aware of the acceptable use of Information Technology with the aim that it is always used in a safe and secure manner. This policy covers all areas of the school including EYFS, before and after school care, holiday clubs and extra-curricular activities. It relates in particular to the use of technology, including:

- the internet
- e-mail
- mobile phones and smartphones
- computers, be they desktops, laptops, netbooks, chromebooks, tablets or other such devices
- personal music players
- devices with the capability for recording and/or storing still or moving images and/or audio
- social networking, micro blogging, blogs, message boards and other interactive web sites
- instant messaging, chat rooms and other similar communication services
- webcams, video hosting sites (such as YouTube)
- gaming sites and devices
- Online cloud based Environments such as Mathletics, Oxford Reading Buddy
- SMART boards, other interactive boards and screens
- Other photographic or electronic equipment.
- Apps
- Podcasting
- On demand TV and video, movies and radio / Smart TVs
- CCTV

It applies to the use of any of the above on school premises and also any use, whether on or off school premises, which affects the welfare of other pupils or where the culture or reputation of the school are put at risk. [Staff are subject to a range of separate detailed policies to cover

the use of technology and working safely more generally, but should pay due regard to this policy].

1.2 AIMS

The aims of this policy are:

1. to encourage pupils to make good use of the educational opportunities presented by access to the internet and other electronic communication;
2. to safeguard and promote the welfare of pupils by preventing cyberbullying and other forms of abuse; within the context of our safeguarding policy.
3. to minimise the risk of harm to the assets and reputation of the School;
4. to help pupils take responsibility for their own e-safety (i.e. limiting the risks that children and young people are exposed to when using technology); see also our PSHEE policy.
5. to ensure that pupils use technology safely and securely.

2. USE OF TECHNOLOGY

2.1 INTERNET AND EMAIL

The School provides internet access and an extensive suite of tools. A pupil can only access the internet when given permission by a member of staff and is under direct supervision at all times. In addition the school uses filtering technology to prevent access to undesirable sites.

Staff must ensure that any films or material that is shown to children are age appropriate.

At Avalon, no children under the age of 13 will have access to services that require a 13+ age requirement. Pupils/Students must enter their true date of birth when/where requested.

Pupils are responsible for their actions, conduct and behaviour on the internet in the same way that they are responsible during classes or at break time. Use of technology should be safe, responsible and legal. If a pupil is aware of misuse by other pupils he/she should talk to a teacher about it as soon as possible. The teacher must report it to the Computing Coordinator who must complete an incident section in the 'Online Safety Log' and follow the procedures as set out in the 'E-Safety Policy'.

Any misuse of the internet will be dealt with under the School's Behaviour Policy. Use of all internet services provided by the school by pupils or parents may be monitored by the school for the purpose of ensuring this policy is being adhered to.

CYBER-BULLYING

Pupils must not use their own or the School's technology to bully others. Bullying incidents involving the use of technology will be dealt with under the School's Anti-bullying Policy.

Current behaviours that fall into this category, often referred to as Cyber-bullying include

- Texting scary or rude messages by electronic devices.
- Sending unpleasant photographs by electronic devices.
- Using online message boards, chat rooms or social networking sites to post cruel messages
- Deleting the victim's name from or ignoring their messages on social networking sites
- Someone taking an indecent image of themselves, and sending it to their friends or boy/girlfriend via a mobile phone or some other form of technology is sometimes referred to as 'sexting'. The creation, possession and transmission of any indecent image containing a person under 18 is illegal, and the school is required to report such incidents to the police. This also includes "upskirting" - taking pictures under a person's clothing without them knowing, with the intention of viewing their genitals or buttocks which is a specific criminal offense.
- Once these images have been taken and sent to others, control is lost of them and they can end up anywhere. They could be seen by friends and family, a future employer, or even, in some cases, end up in the possession of an offender.
- This also puts that person who originally sent the images in a vulnerable position, as somebody they may or may not know now has these images and could use technology to bully, harass or even try to locate them.
- Advice to children in this area should say: "Just think – if you wouldn't print and pass these images around your school or show your mum or dad, they are not appropriate to share via phone or other technologies".
- If there is a suggestion that a child is at risk of abuse or significant harm, the matter will be dealt with under the School's child protection procedures (see the School's Safeguarding Policy). If you are worried about something that you have seen on the internet, talk to a teacher about it as soon as possible.
- Further information can be found https://www.gov.uk/government/groups/uk-council-for-child-internet-safety-ukccis#ukccis-publications

THE COMPUTER MISUSE ACT (1990)

1. No one may access computer material without permission, eg looking at someone else's files.
2. No one may access computer material without permission with intent to commit further criminal offences, eg *hacking* into the bank's computer and wanting to increase the amount in an account.
3. No one may alter computer *data* without permission, eg writing a *virus* to destroy someone else's data, or actually changing the money in an account.

THE DATA PROTECTION ACT (1998) and THE GENERAL DATA PROTECTION REGULATION (GDPR)(2018)

These help to provide protection against the abuse of personal information. No one may collect data without planning to use it sensibly, within reason and store it safely.

The school aims at all times to keep personal data secure. It takes suitable measures to prevent unauthorised or unlawful processing of personal data and accidental loss or destruction of or damage to personal data.

The data controller in the school is responsible for ensuring that personal data stored on school systems regarding staff is appropriately restricted and only accessible to designated individuals.

COPYRIGHT LAW

No one is allowed to misuse other people's creative works, such as by the copying of written, musical, or film works using computers.

USE OF CHILDREN'S NAMES IN EMAIL

Because our data protection policy sets out to ensure that all matters pertaining to a child of interest and public record are to be stored in his/her own file, kept by the school office, we do not want children's names used in emails.

This is specifically important for issues of safeguarding, as communication errors can give rise to inappropriate people gaining access to sensitive information. It is also important that children involved in disciplinary matters are not named in emails, for similar reasons. Avalon School have secure drives where any sensitive or confidential information about a pupil can be stored and only those staff who have need to know are able to see it.

Obviously in matters of team selection for sports or prize winners for assembly, the use of names is necessary for accuracy, but where possible, staff are asked to reduce to a minimum the use of first name/surname of children.

THE LIABILITY OF THE SCHOOL

The school takes reasonable precautions to ensure that pupils cannot access inappropriate material, including the teaching of Internet safety skills to pupils. However, unless negligent under the terms of this policy, the School accepts no responsibility to the pupil or parents

caused by or arising out of a pupil's use of the Internet, e-mail or any electronic device whilst at School.

2.2 ACCESS AND SECURITY

Access to the Internet from the School's computers and network must be for educational purposes only. No-one must use the School's facilities or network for personal, social or non-educational use without the express, prior consent of an appropriately competent member of staff.

No-one must knowingly obtain (or attempt to obtain) unauthorised access to any part of the School's or any other computer system, or any information contained on such a system.

No laptop or other mobile electronic device may be connected to the School network without the consent in writing to the IT Coordinator (L McFerran) or SLT.

All computers in the ICT suite can be accessed with autologon but has been write protected.

All staff and KS2 children have their own logons to the school network. Access to secure drives on the network are given to those staff who have permission as agreed with the SLT. No one should let anyone else know their passwords.

Any sensitive information (eg school reports) held on portable storage devices such as memory sticks, must be password protected.

Access to the server is password protected and only available to the SLT, IT coordinator and maintenance staff as agreed by the IT coordinator (L McFerran) or SLT.

No-one must disable or uninstall any anti-virus software on the School's computers.

No-one must use the School's computer system for anything but educational purposes or to aid in the running of the school.

Where staff are using EY log (or similar system) to track and provide information for parents on their child's progress, the software is stored on school-owned devises and can be used by EYFS authorised personnel only.

Pupils and Staff must take care to protect personal and confidential information about themselves and others when using the internet.

Viewing, retrieving, downloading or sharing any material which in the reasonable opinion of the Head teacher is unsuitable, at any time, is strictly prohibited.

No-one must enter into any contractual commitment using the internet when in the care of the School, or otherwise associated with the School, whether for themselves or on behalf of another (including the School).

If the SLT have reasonable cause to think that a member of staff's device has been used in contravention of this policy or other school policies then the SLT may insist that the device be examined in an unlocked state and if using the school network, their logon folders will be viewed. (For example, inappropriate pictures taken of pupils).

2.3 MOBILE ELECTRONIC DEVICES PROTOCOL

"Mobile electronic device" includes without limitation mobile phones, smartphones, tablets, laptops, MP3 players and wearable technology.

Pupils are not permitted to bring mobile devices to school.

In exceptional circumstance, such as requiring a phone as their parents have given permission for the pupil to walk home, the phone must be brought to the school office on arrival and switched off. The phone can then be collected at the end of the school day. Staff will not take responsibility for the device.

In emergencies, pupils may request to use the School telephone. Parents wishing to contact their children in an emergency should always telephone the School Office and a message will be relayed promptly.

Staff are allowed to bring their own mobile devices into school but should not use them for personal matters when on duty, during these times the mobile devices should be either switched off or on silent.

Staff on school trips may carry and use a mobile phone to seek assistance from colleagues or emergency services. They should always use the school phones where possible and seek permission form the SLT to use their own mobiles.

2.4 PHOTOGRAPHS AND IMAGES

Schools have a duty of care to ensure that any images used are in the right context and are appropriate. Avalon School recognises that the arrival of new technologies and multiple devices means that personal productivity tools such as cameras, phones, tablets and laptops may very well be used by staff and pupils in the legitimate execution of their duties.

Using photographic material of any kind to bully, harass or intimidate others will not be tolerated and will constitute a serious breach of discipline.

All photographs must be taken on school equipment and stored on school devices or the school web-services.

Pupils may only use cameras or any mobile electronic device with the capability for recording and / or storing still or moving images with the express permission of the member of staff in charge and with the permission of those appearing in the image.

CCTV and Webcams

The school uses CCTV for security and safety. A live feed of the CCTV covering the drive and parts of the yard and playground is on display in the school office. Notification of CCTV use is displayed at the front of the school.

We do not use publicly accessible webcams in school.

Webcams may be used to Skype as planned by the teacher and agreed by the SLT. Prior Parental consent must be obtained for any other broadcast on the internet.

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).

Webcams include any camera on an electronic device which is capable of producing video. School policy should be followed regarding the use of such personal devices.

Important points to consider:

Parents are asked to give consent when their child enrols at the school to use their child's image in publicity.

If consent is not given, ensure that all staff are aware and make every effort to comply sensitively. Be careful with inter-school events, it may it may be necessary to liaise with staff from the other school/s.

Try to only take photos of groups of children unless you specifically need to take a picture of an individual child.

Ensure that children are dressed appropriately and that images cannot be construed as provocative.

Where possible, do not use an image of a child who is no longer at the School

Use an image in the intended context only (as stated on the consent form) and do not use it to illustrate sensitive or negative issues.

Do not use images of a child who is considered vulnerable unless parents/carers have given specific written permission.

Regularly review stored images and delete unwanted material.

If consent is not given, ensure that all staff are aware and make every effort to comply sensitively. Be careful with inter-school events, it may it may be necessary to liaise with staff from the other school/s.

Allocate specific times during School outings and educational visits for photographs to be taken in the appropriate setting and areas.

2.5 USE OF CAMERAS AND RECORDING EQUIPMENT BY PARENTS AND GUARDIANS

Parents are welcome to take photographs of their own children taking part in sporting and outdoor events. When an event is held indoors, such as a play or a concert, parents should be mindful of the need to use their cameras and recording devices with consideration and courtesy for the comfort of others.

The school asks parents not to take photographs of other pupils on their own without the prior agreement of that child's parents. If it is impossible to avoid taking pictures or video of other's children due to the nature of the event, such images or video must not be loaded onto social media.

The school also asks parents not to take photographs of their child or his/her fellow pupils in the swimming pool or changing rooms.

Flash photography can disturb others in the audience or even cause distress for those with medical conditions; we therefore ask that it is not used at indoor events.

Parents are also reminded that copyright issues may prevent the school from permitting the filming or recording of some plays and concerts.

2.6 INAPPROPRIATE COMMUNICATIONS

Employees Avalon School are bound by the confidentiality requirements of both their contract and by statute. Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records protected by the Data Protection Act 1998 and 2018.
- Information divulged in the expectation of confidentiality
- School business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations

All staff must be conscious at all times of the need to keep their personal and professional lives separate. At no stage should employees or pupils risk reputational damage to the school through inappropriate use of social media.

Staff should keep their own Social Media identity as locked down and private as possible, so that parents and children at school cannot find out inappropriate information about them or their family.

Staff employees must decline 'friend requests' from pupils they receive in their personal social media accounts. They should not request any personal information from pupils, other than that which might be appropriate as part of their professional role. Adults should ensure that all communications are transparent and open to scrutiny. They should not give out their personal contact details to children including email, home or mobile telephone numbers, unless the need to do so is agreed with senior management.

Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing school uniforms or clothing with school or associated logos from ISA or images identifying sensitive school premises must not be published on personal webspace. Parents and pupils must be specifically careful about publishing on their family spaces pictures of other children in the school, unless they have the permission of the children and families involved. Images shared on social media platforms with families of children by teachers to demonstrate progress made or successes achieved is not permitted. The school has established official social media accounts for the use of promoting the school and the achievements of the children and these are the only accounts that should be used for this purpose.

Caution is advised when inviting work colleagues to be 'friends' in personal social networking sites. Social networking sites blur the line between work and personal lives and it may be difficult to maintain professional relationships or it might be just too embarrassing if too much personal information is known in the work place.

Staff employees must not engage in personal use of social media during employed time.

Staff employees must not edit open access online encyclopedias such as *Wikipedia* in a personal capacity at work. This is because the source of the correction will be recorded as the employer's IP address and the intervention will, therefore, appear as if it comes from the employer itself.

2.7 MONITORING AND REVIEW

All serious e-safety incidents will be logged in the pupil's personal file.

The Governors, in consultation with the Head teacher has responsibility for the implementation and review of this policy, in consultation with parents, pupils and staff. The Governors will consider the record of e-safety incidents and new technologies and will consider if existing security procedures are adequate.

2.8 FURTHER INFORMATION ON SAFE USE OF TECHNOLOGY:

Avalon School Staff Code of Conduct – Communication with Children and Young People.

Avalon School Staff Code of Conduct – Photography and Videos

Avalon School Staff Code of Conduct – Access to Inappropriate Images and Internet Usage.

Avalon School Staff Handbook – Internet and e-mail policy.

E-Safety Policy

APPENDIX 1 - IT ACCEPTABLE USE AGREEMENT

The acceptable use agreement given to all parents for their joint agreement on safe use of the Internet:

E-Safety and the Internet

As part of your child's curriculum and the development of Computing skills, Avalon School provides supervised access to the Internet. We believe that the use of the World Wide Web and Email is worthwhile and is an essential skill for children as they grow up in the modern world. Please would you read the attached Rules for Acceptable Computer Use Policy and talk about them with your child as appropriate to their age. Then sign consent form so that your child may use the Internet at School.

We take positive steps to deal with this any risk of the children in our School having access to undesirable materials, including our Internet provider operating a filtering system that restricts access to inappropriate materials.

Whilst every endeavour is made to ensure that suitable restrictions are placed on the ability of children to access inappropriate materials, the School cannot be held responsible for the nature or content of materials accessed through the Internet. The School will not be liable for any damages arising from your child's use of the Internet facilities.

Our rules also concern the types of communications that children make using computers and other technology. We would like your support in helping to ensure that the children at the School are using technology in a responsible and polite manner and never in a way that could upset another person or spoil their work.

A full copy of our E-safety policy is on the School website or available in School should you require a copy.

Should you wish to discuss any aspect of Internet use please contact Miss McFerran our Computing Coordinator, or you child's class teacher in the first instance.

Please read and discuss with your child then sign and return to the School.

- Children must ask permission before accessing the Internet.
- We expect all children to be responsible for their own behaviour on the Internet, just as they are anywhere else in School. This includes materials they choose to access, and language they use.
- Children must only use websites and search engines as directed by staff.
- Children are expected not to use any rude language in their email communications and contact only people the staff have approved.
- Children should not access other people's files unless permission has been given.
- Computers should only be used for schoolwork and homework unless permission has been granted otherwise.
- No program files may be downloaded to the computer from the Internet.

- No programs on disc, memory drives etc. may be brought in to School and used without approval from staff first.

- Children not complying with these expectations will be warned, and subsequently, may be denied access to Internet resources.

E-Safety and the Internet

Nursery, Pre-School & Infant Children			
I have read through the agreement and gone through it as appropriate with my child and agree to adhere to it. Please sign below on behalf of your child:			
Signed by Parent/Carer:		Date:	

Junior Children			
I have read and understand the School Rules for Responsible Internet Use. I will use the computer system and Internet in a responsible way and obey these rules at all times.			
Signed by Child:		Date:	

Parent's Consent for Internet Access			
I have read and understood the School rules for responsible Internet use and give permission for my child to access the Internet. I understand that the School will take all reasonable precautions to ensure children cannot access inappropriate materials. I understand that the School cannot be held responsible for the nature or content of materials accessed through the Internet. I agree that the School is not liable for any damages arising from use of the Internet facilities.			
Signed by Parent/Carer:		Date:	

APPENDIX 2 - RELATED LEGISLATION

1) ACTS RELATING TO MONITORING OF STAFF EMAIL

Data Protection Act 2018 (incorporating GDPR)

https://www.gov.uk/government/collections/data-protection-act-2018

Data Protection Act 1998

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.

http://www.hmso.gov.uk/acts/acts1998/19980029.htm

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 ESAFETY

Prevent as part of the CTSA Act 2015

From 1 July 2015 all schools are subject to a duty under section 26 of the Counter-Terrorism and Security Act 2015, in the exercise of their functions, to have "due regard to the need to prevent people from being drawn into terrorism". This duty is known as the Prevent duty. It applies to a wide range of public-facing bodies. Bodies to which the duty applies must have regard to the statutory guidance. https://www.gov.uk/government/publications/prevent-duty-guidance Paragraphs 57-76 of the guidance are concerned specifically with schools and childcare providers.

The statutory guidance makes clear the need for schools to ensure that children are safe from terrorist and extremist material when accessing the internet in schools. Schools should ensure that suitable filtering is in place. More generally, schools have an important role to play in equipping children and young people to stay safe online, both in school and outside. Internet safety will usually be integral to a school's ICT curriculum and can also be embedded in PSHE and SRE. General advice and resources for schools on internet safety are available on the UK Safer Internet Centre website. As with other online risks of harm, every teacher needs to be aware of the risks posed by the online activity of extremist and terrorist groups.

Racial and Religious Hatred Act 2006

It a criminal offence to threaten people because of their faith, or to stir up religious hatred by displaying, publishing or distributing written material which is threatening. Other laws already protect people from threats based on their race, nationality or ethnic background.

Sexual Offences Act 2003

The new grooming offence is committed if you are over 18 and have communicated with a child under 16 at least twice (including by phone or using the Internet) it is an offence to meet them or travel to meet them anywhere in the world with the intention of committing a sexual offence. Causing a child under 16 to watch a sexual act is illegal, including looking at images such as videos, photos or webcams, for your own gratification. It is also an offence for a person in a position of trust to engage in sexual activity with any person under 18, with whom they are in a position of trust. Schools should already have a copy of "*Children & Families: Safer from Sexual Crime*" document as part of their child protection packs.

Communications Act 2003 (section 127)

Sending by means of the Internet a message or other matter that is grossly offensive or of an indecent, obscene or menacing character; or sending a false message by means of or persistently making use of the Internet for the purpose of causing annoyance, inconvenience or needless anxiety is guilty of an offence liable, on conviction, to imprisonment. This wording is important because an offence is complete as soon as the message has been sent: there is no need to prove any intent or purpose.

The Computer Misuse Act 1990 (sections 1 – 3)

Regardless of an individual's motivation, the Act makes it a criminal offence to gain:

- access to computer files or software without permission (for example using another person's password to access files)
- unauthorised access, as above, in order to commit a further criminal act (such as fraud)
- impair the operation of a computer or program

UK citizens or residents may be extradited to another country if they are suspected of committing any of the above offences.

Malicious Communications Act 1988 (section 1)

This legislation makes it a criminal offence to send an electronic message (e-mail) that conveys indecent, grossly offensive, threatening material or information that is false; or is of an indecent or grossly offensive nature if the purpose was to cause a recipient to suffer distress or anxiety.

Copyright, Design and Patents Act 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 a 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

Data Protection Act 2018 (incorporating GDPR)

https://www.gov.uk/government/collections/data-protection-act-2018

Data Protection Act 1998

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

The Freedom of Information Act 2000

https://ico.org.uk/for-organisations/guide-to-freedom-of-information/