



Medina House School Social Media Policy

December 2018

Approved by the Governors on

Signed Date:
Chair of Governors

Review Date : December 2019

Contents

Section 1: Introduction	4
1.1 Objectives.....	4
1.2 Scope.....	4
1.3 Status	5
1.4 Principles.....	5
Section 2: Safer Social Media Practice in Schools	5
2.1 What is social media?	5
2.2 Overview and expectations	5
2.3 Safer online behaviour.....	6
2.4 Protection of personal information	7
2.5 Communication between pupils / schools staff	7
2.6 Social contact.....	8
2.7 Access to inappropriate images and internet usage	8
2.8 Cyberbullying	9
Section 3: As an Assessment Tool	8
Section 4: Business use of Social Media	8
Section 5: Link with other policies	10
Section 6: Review of Policy	11
Section 7: Appendices	12
Appendix A - Staff Guide to facebook.....	12
Appendix B - Staff guide to usage of Mobile Phones.....	13
Appendix C – Relevant legislation	14

Section 1: Introduction

1.1 Objectives

1.1.1 This policy sets out the School's policy on social networking. New technologies are an integral part of our lives and are powerful tools which open up teaching and learning opportunities for schools' staff in many ways. This policy sets out Medina House School's policy on social networking and aims to:

- **Assist the school's staff working with children to work safely and responsibly with the internet and other communication technologies and to monitor their own standards and practice**
- **Set clear expectations of behaviour and/or codes of practice relevant to social networking for educational, personal or recreational use**
- **Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken**
- **Support safer working practice**
- **Minimise the risk of misplaced or malicious allegations made against adults who work with pupils**
- **Reduce the incidence of positions of trust being abused or misused**

1.1.2 Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities. There may be times when professional judgements are made in situations not covered by this document, or which directly contravene the standards outlined in this document. It is expected that in these circumstances staff in the school will always advise the headteacher of the justification for any such action already taken or proposed. The Headteacher will in turn seek advice from the School's HR provider where appropriate.

1.1.3 This policy takes account of employment legislation and best practice guidelines in relation to social networking in addition to the legal obligations of governing bodies and the relevant legislation listed at appendix A.

1.2 Scope

1.2.1 This document applies to all staff who work at Medina House School as adopted by the Governing body. This includes teachers, support staff, supply staff, governors, contractors, people on work-experience and volunteers.

1.2.2 It should be followed by any adult whose work brings them into contact with pupils. References to staff should be taken to apply to all the above groups of people in the school. Reference to pupils means all pupils at the school.

1.2.3 This policy should not be used to address issues where other policies and procedures exist to deal with them. For example any alleged misconduct which falls within the scope of the Staff Discipline Policy or the Allegations of Abuse Against School Staff Policy, which requires the school to comply with additional child protection requirements as set out in that policy

1.3 Status

1.3.1 This document does not replace or take priority over advice given by the school's codes of conduct, dealing with allegations of abuse, other policies issued around safeguarding or IT issues (email, ICT

and data protection policies), but is intended to both supplement and complement any such principles.

- Adults who work with pupils are responsible for their own actions and behaviour and should avoid any conduct which would lead any reasonable person to question their motivation and intentions.
- Staff in schools should work and be seen to work, in an open and transparent way.
- Staff in schools should continually monitor and review their practice in terms of the continually evolving world of social networking and ensure they follow the guidance contained in this document.

Section 2: Safer Social Media Practice in Schools

2.1 What is social media?

- 2.1.1 For the purpose of this policy, social media is the term commonly used for websites which allow people to interact with each other in some way – by sharing information, opinions, knowledge and interests. Social networking websites such as Facebook, bebo and MySpace are perhaps the most well known examples of social media but the term also covers other web based services such as blogs, video and audio podcasts, wikis, message boards, photo document and video sharing websites such as YouTube and micro blogging services such as Twitter. This definition of social media is not exhaustive as technology develops with new ways of communicating advancing every day.
- 2.1.2 For the purpose of this document the terminology Social Media is not exhaustive and also applies to the use of communication technologies such as mobile phones, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

2.2 Overview and expectations

- 2.2.1 All adults working with pupils have a responsibility to maintain public confidence in their ability to safeguard the welfare and best interests of pupils. It is therefore expected that they will adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, pupils or students, public in general and all those with whom they work in line with the school's code of conduct. Adults in contact with pupils must therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
- 2.2.2 The guidance contained in this policy is an attempt to identify what behaviours are expected of school staff who work with pupils. Anyone whose practice deviates from this document and/or their professional or employment-related code of conduct may bring into question their suitability to work with children and young people and will result in disciplinary action being taken against them.
- 2.2.3 School staff must always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other communication technologies, which might be misinterpreted by others. They must report and record any incident with this potential.

2.3 Safer online behaviour

- 2.3.1 Managing personal information effectively makes it far less likely that information will be misused.
- 2.3.2 In their own interests, staff need to be aware of the dangers of putting personal information onto social networking sites, such as addresses, home and mobile phone numbers. This will avoid the potential for pupils or their families or friends having access to staff outside of the school environment. It also reduces the potential for identity theft by third parties.

- 2.3.3 All staff, particularly new staff, should review their social networking sites when they join the school to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and the school if they are published outside of the site.
- 2.3.4 Staff must never 'friend' any pupil. It is accepted that there may be exceptions where people move in the same social circles. To avoid misunderstanding, the Headteacher must be informed in such cases.
- 2.3.5 Staff must never use or access social networking sites of pupils and must never accept an invitation to 'friend' a pupil.
- 2.3.6 Confidentiality needs to be considered at all times. Social networking sites have the potential to discuss inappropriate information and employees need to ensure that they do not put any confidential information on their site about themselves, their employer, their colleagues, pupils or members of the public.
- 2.3.7 Employees need to ensure that when they are communicating about others, even outside of work, that they give due regard to the potential for defamation of character. Making allegations on social networking sites (even in their own time and in their own homes) about other employees, pupils or other individuals connected with the school, or another school, or the Local Authority could result in formal action being taken against them.
- 2.3.8 Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.
- 2.3.9 Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring the school or its community into disrepute.
- 2.3.10 Some social networking sites and other web-based sites have fields in the user profile for job title etc. If you are an employee of a school and particularly if you are a teacher, you should not put any information onto the site that could identify either your profession or the school where you work. In some circumstances this could damage the reputation of the school, the profession or the local authority.
- 2.3.11 Staff are reminded that they should not connect their own personal devices to the school network or wifi network.

2.4 Protection of personal information

- 2.4.1 Staff must ensure that they do not use school ICT equipment for personal use, e.g. camera or computers.
- 2.4.2 Staff must keep their personal phone numbers private and not use their own mobile phones to contact pupils or parents.
- 2.4.3 Staff must never share their work log-ins or passwords with other people.
- 2.4.4 Staff must not give their personal e-mail addresses to pupils or parents. Where there is a need for homework to be sent electronically the school e-mail address must be used.
- 2.4.5 Staff must keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on school premises.
- 2.4.6 Staff are advised to understand who is allowed to view the content on their pages of the sites they use and how to restrict access to certain groups of people.

2.5 Communication between pupils / schools staff

- 2.5.1 Communication between pupils and staff, by whatever method, must take place within clear and explicit professional boundaries.
- 2.5.2 This includes the wider use of technology such as mobile phones, text messaging, e-mails, digital cameras, videos, web-cams, websites and blogs.
- 2.5.3 It is the expectation that the school will provide a work mobile and e-mail address for communication between staff and pupils. Staff must not give their personal mobile numbers or personal e-mail addresses to pupils or parents. Staff undertaking direct payment work must inform the Headteacher.
- 2.5.4 Staff must not request, or respond to, any personal information from a pupil, other than that which might be appropriate as part of their professional role.
- 2.5.5 Staff should ensure that all communications are transparent and open to scrutiny. They must also be circumspect in their communications with pupils so as to avoid any possible misinterpretation of their motives or any behaviour which could be construed as 'grooming' in the context of sexual offending.
- 2.5.6 Staff must not give their personal contact details to pupils including e-mail, home or mobile telephone numbers, unless the need to do so is agreed with senior management and parents/carers.
- 2.5.7 E-mail or text communications between an adult and a pupil outside agreed protocols will lead to disciplinary action and/or possible criminal investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the school's policy.

2.6 Social contact

- 2.6.1 Staff must not establish or seek to establish social contact via social media / other communication technologies with any pupil for the purpose of securing a friendship or to pursue or strengthen a relationship.
- 2.6.2 There will be occasions when there are social contacts between pupils and staff, where for example the parent and teacher are part of the same social circle. These contacts however, will be easily recognised and openly acknowledged.
- 2.6.3 There must be awareness on the part of those working with pupils that some social networking contacts, especially where these are not common knowledge, can be misconstrued as being part of a grooming process. This can also apply to social networking contacts made through outside interests or through the staff member's own family.

2.7 Access to inappropriate images and internet usage

- 2.7.1 There are no circumstances that will justify adults possessing indecent images of children. Staff who access and possess links to such websites will be viewed as a significant and potential threat to children. Accessing, making and storing indecent images of children is illegal. This will lead to criminal investigation and, if proven, lead to dismissal and the individual being barred from working with children.
- 2.7.2 Staff must not use equipment belonging to the school/service to access any pornography; neither must personal equipment containing these images or links to them be brought into the workplace. This will raise serious concerns about the suitability of the adult to continue to work with children and will lead to dismissal.

- 2.7.3 Adults must ensure that pupils are not exposed to any inappropriate images or web links. The school's staff need to ensure that internet equipment used by pupils have the appropriate controls with regards to access. e.g. personal passwords must be kept confidential. In the event of an inappropriate image appearing, a report must be made immediately to the ICT Co-ordinator, Deputy Head or IT Manager and an entry made in the register held in the main school office.
- 2.7.4 Where indecent images of children are found by staff, it must be immediately reported to the Headteacher (or in her absence the deputy head) who will notify the police and local authority designated officer (LADO). Schools should refer to the dealing with allegations of abuse against staff policy and should not attempt to investigate the matter or evaluate the material themselves, as this may lead to evidence being contaminated which in itself can lead to a criminal prosecution.
- 2.7.5 Where other unsuitable material is found, which may not be illegal but which raises concerns about that member of staff, the Headteacher will inform HR and/or the LADO and seek advice. The school should refer to the dealing with allegations of abuse against staff policy and must not attempt to investigate or evaluate the material themselves until such advice is received.

2.8 Cyberbullying

- 2.8.1 Cyberbullying can be defined as 'the use of modern communication technologies to embarrass, humiliate, threaten or intimidate an individual in the attempt to gain power and control over them.'
- 2.8.2 Prevention activities are key to ensuring that staff are protected from the potential threat of cyberbullying. All employees are reminded of the need to protect themselves from the potential threat of cyberbullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.
- 2.8.3 If cyberbullying does take place, employees should keep records of the abuse, text, e-mails, website or instant message and should not delete texts or e-mails. Employees are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
- 2.8.4 Staff may wish to seek the support of their trade union or professional association representatives or another colleague to support them through the process-
- 2.8.5 Staff are encouraged to report all incidents of cyberbullying to their line manager or the headteacher. All such incidents will be taken seriously and will be dealt with in consideration of the wishes of the person who has reported the incident. It is for the individual who is being bullied to decide whether they wish to report the actions to the police.

Section 3: As an Assessment Tool

3.1 Social media accounts are a good way of having a better understanding of an individual's life and there may be justification for accessing someone's personal social media accounts if they are open source material.

3.2 Social media accounts give an opportunity to see beyond what and how individuals present to professionals during assessment visits.

3.3 It could be considered proportionate to view an individual's social media account to seek evidence to confirm or refute something that may be a concern (child safeguarding). This decision should be made on a case by case basis with a recorded view why this is being done, by whom and should always consider who is best placed to do it. If done from a personal account you run the risk of leaving a digital footprint for that individual to know you have accessed their information, therefore this should only be done from an organisational device/account and before doing this individuals should seek line manager approval for doing this and the rationale should be clearly recorded. This should **only** be done for concerns of a child protection nature and not 'to be nosy'.

3.4 Organisations who wish to do this should consider including a reference to it in their information sharing policy that... *"In order to protect your child(ren) and provide the best possible service, we may sometimes need to gather information from other agencies and sources both on and off-line."*

3.5 If an organisation or its workforce do view a service user's social media account and there is relevant information to a child protection concern on there, they may consider taking a screenshot of this. Screenshots have previously been admissible in court as evidence. That a screenshot has been taken should be recorded in the service user record, by whom and for what purpose, along with information gleaned and a copy of the screenshot.

3.6 No individual's social media account should **ever** be 'hacked'.

3.7 Practitioners should **never** link their personal accounts to other individuals they are working with, with a view to taking a look at that individual's personal information and posts, because this in turn could allow other people to see their own information.

Section 4: Business Use of Social Media

4.1 Writing for council social media profiles

- The purpose will be to provide or promote some form of information to a specific or general audience.
- The information provided should be clear, accurate and fair - and not misleading.
- The media may deem the content of council social media profiles/accounts to be official comment, so take care with any material placed online.
- If posting in response to a comment on a council profile/account, any contribution should be designed to add value in a relevant way and be careful to avoid getting into an argument or inflaming a discussion. If you are unsure of how to respond, contact the media team before responding.
- You should not do anything to jeopardise Isle of Wight Council copyrightable material, confidential information and intellectual property through the use of social media. Further information can be found via the [Employee Code of Conduct](#).
- Avoid misappropriating or infringing the intellectual property of other companies and individuals, which can create liability for the organisation, as well as the individual author.
- Do not use council logos, slogans or other trademarks, or post any of our confidential information without prior written permission from the media team.
- Where appropriate, ensure that you reference sources of particular information (posted or uploaded) and cite them accurately to protect against liability for copyright infringement.
- When linking from your business social media page to any external websites, you should post this disclaimer:

4.2 Moderation guidelines

- Posts on our social media sites will not be moderated before they appear.
- If we become aware of a published post that is in breach of our guidelines then we reserve the right to delete it as we see appropriate.
- Posts with objectionable content will be deleted as opposed to any content being edited out.

- Posts in languages other than English should be avoided as we do not have the facility to moderate these (the council reserves the right to remove such posts).
- If you post a comment which is removed and you do not believe it is in breach of the guidelines, please contact us via www.iwight.com/media
- If you have any questions about these guidelines, please contact us via www.iwight.com/media
- Due to the increased use of Social Media, these guidelines will be updated frequently if required.

4.3 Prohibited content

Please ensure you do not post any material that:

- is abusive, obscene, indecent, discriminatory or offensive;
- is defamatory, harassing or hateful and capable of damaging the reputation of a person or organisation;
- invades anyone's privacy or impersonates anyone;
- encourages conduct that may or would constitute a criminal offence, give rise to civil liability or violate any other law;
- includes personal information of others, such as name, address, place of employment, contact details or professional role;
- includes inappropriate user names that are vulgar or offensive;
- is far off-topic (irrelevant posts that devalue debate for other users may be removed);
- contains irrelevant or excessive links or appears to contain code;
- constitutes spam, unauthorised advertising or which may solicit such material;
- contains long, embedded weblinks;
- contains logos, slogans or other trademarks;
- includes a writing style or language that is against the council's [Plain English Guide](#);
- is political or which contains links to overtly political sites (this is especially relevant in pre-election periods);
- contains confidential information;
- may breach copyright law or infringe intellectual property.

Section 5: Link with other policies

5.1.1 This policy should be read in conjunction with the following documents:

- E- Safety Guidance
- Single Equality Policy
- Whistleblowing Policy
- Safer Recruitment and Safeguarding Children 2012
- * Staff Discipline Policy
- * Freedom of Information Policy
- * Child Protection Policy

5.1.2 All employees must adhere to, and apply the principles of the policy in all aspects of their work. Failure to do so will lead to action being taken under the disciplinary procedure.

Section 6: Review of policy

6.1.1 Due to the ever changing nature of information and communication technologies it is best practice that this policy be reviewed annually and, if necessary, more frequently in response to any significant new developments in the use of technologies, new threats to e-safety or incidents that have taken place.

Section 7: Appendices

Appendix A –



Staff Guide to Facebook

Here are some suggested guidelines for using facebook safely:

- Ensure that all your privacy setting are set to 'Friends Only'. Go to your Account Settings and make sure that the Custom Settings are highlighted and that these show that status, photos and posts are set to 'Friends Only'.
- Consider what information you have on your info page and your profile picture. Don't share personal information that you wouldn't share in class and don't bad mouth anyone.
- If you have professional and social 'friends' on Facebook, using the group list feature will ensure that you can distinguish what type of information you send to particular groups. Make sure that you do not accept pupils (even those that have recently left the school), parents or carers as 'friends'.
- Ensure that you do not bring your professional status and educational institute into disrepute. Make sure that you consider what you post about colleagues, pupils or parents, the school or the Isle of Wight Council. Taking charge of your digital reputation is important, as unprofessional posts or images will lead to disciplinary action and possible failure to gain employment in the future.
- Be careful what photographs you include on your profile. Once these are uploaded, they are very difficult to remove and, using image editing software, they can be altered and merged with other distasteful images. Don't have an unprofessional profile picture, e.g. a sunset, will assist in making your profile indistinctive.
- Be aware of any spam or potential virus risks sent via rogue posts. It is advisable to check with anti-virus firms if you get any suspicious requests or posts.
- If you are alerted to any negative or unscrupulous information about yourself, colleagues or the school on Facebook, inform the Headteacher. Further advice to help with cyberbullying incidents etc, can be gained from a professional association such as your Trade Union.



Appendix B

Staff Guide to usage of Mobile Phones

The following rules apply for the use of personal mobile phones:

- Children are **not** permitted to bring mobile phones to school.
- The school accepts that employees will bring their mobile phones to work.
- As a general rule, employees are not permitted to make/receive calls/texts or go on facebook/internet during work time (excluding break time).
- Staff should ensure that mobile phones are turned off or on silent at all times while on school premises. They should be kept in a cupboard or bag and not be left on display.
- In the event that an employee has a particular reason for a specified period of time, they may request via the manager that they leave their phone on during working hours.
- Staff are **not at any time** permitted to use recording equipment on their mobile phones, i.e. taking photographs or videos of children.
- Staff are not permitted to give their personal mobile phone numbers to children or parents.
- Mobile phones must never be used in a space where children are present (e.g. Classroom, playground, corridors etc).

Offsite trips

- Whilst on off-site trips the allocated emergency mobile i.e. the phone number on the Evolve form, **must** be left on so that school contact can be maintained at any time.
- Whilst off-site this phone must only be used to make contact with school and or to relevant services in the event of an emergency.
- The same rules regarding recording pupils apply off-site i.e. mobile phones **must not** be used to take photos/videos during off-site trips.

Contractors

Contractors will be expected to follow the following procedures whilst on site:

- Mobile phones will only be used to contact their work base as per individual company policy
- Mobile phones will **not** be used to take photos/videos of children/staff.
- If photos need to be taken of the work in line with company policy, permission will need to be obtained from the Headteacher.

Other related Policies

See [Social Media Policy](#)

Appendix C – Relevant legislation

Schools staff should be aware of the legislative framework which currently surrounds use of social media / communication technology in the UK. It is important to note that in general terms an action that is illegal if committed offline is also illegal if committed online.

Equality Act 2010

There are now 9 protective characteristics to provide for equality of access to employment, goods and services:

- Age
- Disability
- Gender reassignment – gender identity
- Marriage and civil partnership
- Pregnancy and maternity
- Race
- Religion/ belief
- Sex
- Sexual orientation

Computer misuse act 1990

This Act makes it an offence to:

- Erase or amend data or programs without authority;
- Obtain unauthorised access to a computer;
- “Eavesdrop” on a computer;
- Make unauthorised use of computer time or facilities;
- Maliciously corrupt or erase data or programs;
- Deny access to authorised users.

Data protection act 1998

This protects the rights and privacy of individual’s data. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully. The Act states that personal data must be:

- Fairly and lawfully processed;
- Processed for limited purposes;
- Adequate, relevant and not excessive;
- Accurate;
- Not kept longer than necessary;
- Processed in accordance with the data subject’s rights;
- Secure;
- Not transferred to other countries without adequate protection.

Freedom of information act 2000

The Freedom of Information Act gives individuals the right to request information held by public authorities. All public authorities and companies wholly owned by public authorities have obligations under the Freedom of Information Act. When responding to requests, they have to follow a number of set procedures.

Communications act 2003

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.

Malicious communications act 1988

It is an offence to send an indecent, offensive, or threatening letter, electronic communication or other article to another person.

Regulation of investigatory powers act 2000

It is an offence for any person to intentionally and without lawful authority intercept any communication. Monitoring or keeping a record of any form of electronic communications is permitted, in order to:

- Establish the facts;
- Ascertain compliance with regulatory or self-regulatory practices or procedures;
- Demonstrate standards, which are or ought to be achieved by persons using the system;
- Investigate or detect unauthorised use of the communications system;
- Prevent or detect crime or in the interests of national security;
- Ensure the effective operation of the system.
- Monitoring but not recording is also permissible in order to:
- Ascertain whether the communication is business or personal;
- Protect or support help line staff.
- The school reserves the right to monitor its systems and communications in line with its rights under this act.

Trade Marks act 1994

This provides protection for Registered Trade Marks, which can be any symbol (words, shapes or images) that are associated with a particular set of goods or services. Registered Trade Marks must not be used without permission. This can also arise from using a Mark that is confusingly similar to an existing Mark.

Copyright, designs and patents act 1988

It is an offence to copy all, or a substantial part of a copyright work. There are, however, certain limited user permissions, such as fair dealing, which means under certain circumstances permission is not needed to copy small amounts for non-commercial research or private study. The Act also provides for Moral Rights, whereby authors can sue if their name is not included in a work they wrote, or if the work has been amended in such a way as to impugn their reputation. Copyright covers materials in print and electronic form, and includes words, images, and sounds, moving images, TV broadcasts and other media (e.g. youtube).

Telecommunications act 1984

It is an offence to send a message or other matter that is grossly offensive or of an indecent, obscene or menacing character. It is also an offence to send a message that is intended to cause annoyance, inconvenience or needless anxiety to another that the sender knows to be false.

Criminal justice & public order act 1994

This defines a criminal offence of intentional harassment, which covers all forms of harassment, including sexual. A person is guilty of an offence if, with intent to cause a person harassment, alarm or distress, they: -

- Use threatening, abusive or insulting words or behaviour, or disorderly behaviour; or

- Display any writing, sign or other visible representation, which is threatening, abusive or insulting, thereby causing that or another person harassment, alarm or distress.

Racial and religious hatred act 2006

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

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.

Protection of children act 1978

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.

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) and you arrange 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 any sexual activity with any person under 18, with whom they are in a position of trust. (Typically, teachers, social workers, health professionals, connexions staff fall in this category of trust). Any sexual intercourse with a child under the age of 13 commits the offence of rape.

Public order act 1986

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. Children, Families and Education Directorate page 38 April 2007.

Obscene publications act 1959 and 1964

Publishing an "obscene" article is a criminal offence. Publishing includes electronic transmission.

Human rights act 1998

This does not deal with any particular issue specifically or any discrete subject area within the law. It is a type of "higher law", affecting all other laws. In the school context, human rights to be aware of include:

- The right to a fair trial
- The right to respect for private and family life, home and correspondence
- Freedom of thought, conscience and religion
- Freedom of expression
- Freedom of assembly
- Prohibition of discrimination
- The right to education

These rights are not absolute. The school is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation