Jesson's CE Primary School
Social Networking Policy

This policy sets out the Jesson's CE Primary School policy on social networking and applies within work and to behaviours outside the work environment. New technologies are an integral part of our lives and are powerful tools which open up opportunities and challenges for staff and volunteers and organisations in many ways. This document aims to:

- Assist 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 and details the aspects of safer online behaviour
- Give a clear message that unlawful or unsafe behaviour is unacceptable and that, where appropriate, disciplinary or legal action will be taken
- Minimise the risk of misplaced or malicious allegations made against staff or volunteers who work with children and young people.
- Prevent adults abusing or misusing their position of trust

Whilst every attempt has been made to cover a wide range of situations, it is recognised that this policy cannot cover all eventualities.
This policy takes account of employment legislation and best practice guidelines in relation to social media.

What is social media?

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. This will also include the use of communication technologies such as smart &mobile phones, tablets, cameras, PDAs / PSPs or other handheld devices and any other emerging forms of communications technologies.

All staff are expected to adopt high standards of personal conduct in order to maintain the confidence and respect of their colleagues, children and young people, and public in general and all those with whom they work across all the business streams. Adults in contact with children and young people should therefore understand and be aware that safe practice also involves using judgement and integrity about behaviours in places other than the work setting.
All staff within their work setting should always maintain appropriate professional boundaries and avoid behaviour, during their use of the internet and other capable devices.

Online behaviour

Managing personal information effectively makes it far less likely that information will be misused.
1. 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 children, young people or their families or friends having access to the adult outside of the work environment. It also reduces the potential for identity theft by third parties.
2. All staff should review their membership of social networking sites to ensure that information available publicly about them is accurate and appropriate. This includes any photographs that may cause embarrassment to themselves and or Jesson's CE Primary School if they are published outside of the site or are accessible to others via their 'page'.
3. 'Friendships' with children of colleagues/family or their own children's friends must be subject to the same level of expectations of behaviour set out in this document.

4. Confidentiality needs to be applied at all times. Social networking sites have the potential to discuss inappropriate information.
5. Staff should ensure that they do not put any confidential information on a site about themselves, their employer, their colleagues, children and young people or members of the public.
6. Staff 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, children, young people or other individuals connected with the Jesson's CE Primary School could result in formal action being taken against them.
7. Staff are also reminded that they must comply with the requirements of equalities legislation in their on-line communications.
8. Staff must never post derogatory remarks or offensive comments on-line or engage in on-line activities which may bring Jesson's CE Primary School into disrepute or could reflect negatively on their professionalism.
9. Some social networking sites and other web-based sites have fields in the user profile for job title etc. Staff should not put any information onto the site that could identify Jesson's CE Primary School as where they work.

Protection of personal information
Staff should:

- Ensure that they do not use Jesson's CE Primary School IT equipment for unauthorised personal use, e.g. camera, phones, laptops or computers.
- Keep their personal phone numbers private and not use their own mobile phones to contact children, young people
- Mobile phones or recording equipment may not be taken into the classrooms or areas where pupils are working without the permission of the Headteacher.)
- Never share their work log-ins or passwords with other people.
- Never give their personal e-mail addresses to children, young people or parents.
- Keep a record of their phone's unique international mobile equipment identity (IMEI) number and keep their phone secure whilst on Jesson's CE Primary School premises.
- 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.

Communication between children, young people and staff
1. Communication between children, young people and adults by whatever method, should take place within clear and explicit professional boundaries.
2. This includes the wider use of technology such as smart and mobile phones, text messaging, e-mails, digital cameras, tablets, Skype etc., videos, web-cams, websites and blogs.
3. Jesson's CE Primary School may provide a work mobile and e-mail address for communication between adults and children/young people where this is necessary for particular reasons.
4. Staff should not request, or respond to, any personal information from a child/young person, other than that which might be appropriate as part of their professional role.
5. Staff should ensure that all communications are transparent and open to scrutiny. They should also be circumspect in their communications with children/young people 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.
6. E-mail or text communications between an adult and a child/young person outside agreed protocols may lead to disciplinary investigations. This also includes communications through internet based web sites. Internal e-mail systems should only be used in accordance with the Jesson's CE Primary School policy.

Social contact
1. Staff should not establish or seek to establish social contact via social media / other communication technologies with children or young people known via their professional/volunteering capacity other than through our own Jesson's CE Primary School Social networking pages.

2. There will be occasions when there are social contacts between children/ young people and staff, where for example the parent and staff member are part of the same social circle. These contacts however, will be easily recognised and should be openly acknowledged where there may be implications for the staff member and their position within the Jesson's CE Primary School setting.

Cyber Bullying

1. Cyber bullying 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. Prevention activities are key to ensuring that staff members are protected from the potential threat of cyber bullying. All staff are reminded of the need to protect themselves from the potential threat of cyber bullying. Following the advice contained in this guidance should reduce the risk of personal information falling into the wrong hands.
3. If cyber bullying 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. Staff are advised to take screen prints of messages or web pages and be careful to record the time, date and place of the site.
4. Staff are encouraged to report all incidents of cyber bullying to their line manager. 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.

Access to inappropriate images and internet usage

1. There are no circumstances that will justify staff 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 disciplinary action being taken as gross misconduct.
2. Staff should not use equipment belonging to Jesson's CE Primary School to access any adult pornography; neither should personal equipment containing these images or links to them be brought into the workplace. Accessing any such images within work time will be subject to the Disciplinary Procedures and will lead to disciplinary action being taken and will raise serious concerns about the suitability of the Staff member continue to work with children.
3. Staff should ensure that children/young people are not exposed to any inappropriate images or web links. Managers need to ensure that internet equipment used by children/young people have the appropriate controls with regards to access e.g. personal passwords should be kept confidential.
4. Where indecent images of children are found, the police and Headteacher of Jesson's CE Primary School should be immediately informed. The Safeguarding and Child Protection procedures should be followed and no 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.
5. Where other unsuitable material is found, which may not be illegal but which raises concerns about a staff member the Headteacher should be informed and advice sought.

Internet Conduct

Our overarching aim is to protect and develop young people, the continued expansion of social network sites make it very difficult to police what information is out there on the World Wide Web. Therefore we are setting out these conduct pointers to assist staff and volunteers to understand and follow our guidance on the use of the internet.

- Whether staff are using the main site page, or the their own personal Facebook or other social media site, staff are reminded that in the public domain they are representing Jesson's CE Primary School and are therefore positive role models to young people. Therefore staff should refrain from posting inappropriate photos, comments, postings and general information to any site. Any such inappropriate data posted will be assessed and if deemed necessary may be taken to a disciplinary process and may ultimately lead to dismissal.
- We do wish to use social media to interface with young people/parents as we see this as a positive way of communication, but we would ask staff to be aware of what might cause offence or bring Jesson's CE Primary School in its broadest sense into disrepute. If you are unsure of a potential posting or become aware of a posting that is inappropriate please report the posting (with hard copy if possible) to the Headteacher.

Link with other policies

1. This document should be read in conjunction with Jesson's CE Primary School relevant policies on;

- Disciplinary Policy and Procedures
- Equal Opportunities Policy
- Staff Code of Conduct

All staff must adhere to, and apply the principles of this document in all aspects of their work and to behaviour outside the work environment. Failure to do so may lead to action being taken under the disciplinary procedure.

Relevant Legislation

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. The following Acts of Parliament apply or acts that may have superseded them:

Computer misuse act

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

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

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
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
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

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.

Trade Marks Act

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

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

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

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

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

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

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

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.

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

Human rights act

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. Jesson’s CE Primary School is obliged to respect these rights and freedoms, balancing them against those rights, duties and obligations, which arise from other relevant legislation.

Date of Governing Body approval: 27.02.18
Date of review: February 2019