Doncaster
Metropolitan Borough Council

Guidance on Social Media Use for Education Establishments

Person Responsible For Policy:	
Approved:	**Date:**
Signed:	**Role:**
To be reviewed:	

Note

This guidance has been drafted by Doncaster Metropolitan Borough Council
The law stated in this guidance is that in force on 1 September 2013.
This guidance only summarises advice and areas of law and does not cover all issues which may be relevant to a particular situation. It is not a substitute for obtaining professional advice on legal and HR issues that may rise within your school.

Contents

Appendices

1. Introduction

Social media is a useful tool for communications. It is an effective means to encourage participation, engagement and sharing. Every public body, including education establishments do need to consider its use as a positive resource. However it very easy for it to be misused or to be used as a tool to attack others particularly with the post now - think later culture. There is also an increasingly blurred line between professional and personal relationships. This guidance will give you information on how to safeguard professionals and your education establishment, as well as children and the school community.

Key points are:

- All users should be aware that posts are not private and are considered in the public domain
- All users should always remember that online participation results in the comments being permanently available and open to being republished in other media.
- All users should make sure that they stay within the legal framework and be aware that libel, defamation, copyright and data protection laws apply.

Key statistics are (at 2013 approximately):

- 85% of UK households have an internet connection.
- 67% of internet users access social networking sites every day.
- 20% of all time spent online is on social media (an average of 61 minutes per day).

Main social network sites:

- Twitter: 33 million accounts in UK (2013) 200 million worldwide.
- Facebook: 34 million accounts in UK (2013) 1 billion worldwide.
- YouTube: 55% of people watch YouTube videos every day - it is estimated that video will account for 57% of consumer internet traffic by 2015 – nearly four times as much as regular web browsing and email. (Pictures and video are key ways to promote engagement on social media).

2. Guidance for secondary education establishments on using social media as a communication tool.

There are many excellent examples of education establishments using Facebook or Twitter to communicate with parents and let others know what is happening at their education establishment. Social media will increasingly become an important part of everyday life.
However it is recommended that the education establishment considers the following before commencing using social media to communicate:

- Who is responsible for monitoring content and posting?
- Ensure the education establishment owns the social media site and access is linked to one or two individual members of staff and passwords are known by only these members of staff.
- Establish terms of use on posting information for staff, pupils and parents.
- It is to be used for education establishment information purposes only and to not be misunderstood and used as a complaints service.
- Prohibit unacceptable postings (defamatory, discriminatory, offensive, threatening, harassing or in breach of copyright, Intellectual Property (IP) or confidence).
- Allow the education establishment to remove posts at its discretion and block members.
- Ensure comments are monitored and issues are dealt with quickly. Please be aware that the busiest time for students and parents to post would be in an evening therefore the staff allocated to monitor the profile should be given adequate time preferably in the mornings.
- You may consider a whole education establishment policy on social media covering acceptable pupil use.
- Ensure compliance with data protection – do not publish photos of children unless you have the signed consent of their parent. An annual opt in including publishing on the education establishment website is advisable.
- If any images of children are to be put onto the education establishments online profile please ensure consent has been given and signed by parents/carers (even if a child is only in the background of an image).
- Make sure the 'tagging function' is enabled on the site, this will ensure children can't tag anybody in the photographs uploaded, unless they have been approved by the members of staff who monitor the site.
- Education establishments need to safeguard children who need protection from being published on social media sites. For further information please see link below:
  http://doncasterscb.proceduresonline.com/chapters/p_photo_young.html

Appendix 1 contains a draft Social Media Policy that an education establishment can adapt.
Appendix 3 also includes Social Media Policy for education establishment staff.

3. Guidance for education establishments in recruitment

Social media is increasingly used to check candidates' before offering a job.

If information on social networks is used to reject candidates then an inference of discrimination can be drawn if that information refers to a protected characteristic under the Equality Act 2010 (including marital status, sexual orientation, age, relations belief or ethnic origin).

It is important that the recruitment process and paper trail shows that appropriate decisions were made.

For further information on safer recruitment please see the link below:

http://www.education.gov.uk/aboutdfe/statutory/g00213145/safeguarding-children-safer-recruitment

Further advice can be obtained from DMBC Legal services 01302 734631.

4. Guidance for education establishments as an employer

It is important that education establishments introduce social media guidance for their employees particularly with regard to the following:

- Employers can be liable for the harassment of employees by other employees if this occurs in the course of employment. Employees are often online 'friends' with their colleagues. If concerning behaviour is happening online it may be happening in the workplace – don't ignore issues.
- All staff in education establishments should be aware of their personal use of social media. In 2011 more than 40 teachers were referred to GTC for unprofessional online conduct. Many teachers have experienced negative conduct/cyber-bullying though social media.
- Staff are reminded of boundaries and are adhere to the responsibilities contained within the Local Authorities model code of conduct

It is advised that:

- Education establishments ensure that contracts of employment refer to the Social Media Policy and a policy is drafted covering the use of social media for employees. (Copy of a draft policy is attached at appendix 3).
  Education establishments could consider the following:
  - Warning on offensive, obscene, discriminatory or harassing online behaviour.
  - Warning on derogatory comments on other staff, pupils or parents.
  - Misuse of confidential, sensitive, personal or copyrighted information.
  - Guidance for in or out of work time.
  - Block pupils as friends.
  - Consideration of colleagues as friends.
  - Rules on privacy settings.
  - Ban on use in work time.
  - Consequence of breach of policy and link to other policies.

- You should ensure that each member of staff is aware of the education establishments Social Media Policy.
- If the education establishment encourages the positive use of social networking sites as part of the educational process, it should provide clear guidance on what is considered to be appropriate contact with students. Having a thorough policy in place will help staff and students to keep within reasonable boundaries
- All must understand that social network sites are not private and are not considered outside the work domain.
- There is a significant risk of damage to the reputation of an education establishment and teacher and damage to careers when inappropriate content is inputted online.
- All Staff should be aware of the role of the LADO (Local Authority Designated Officer for Safeguarding).
- Employers can take action (including dismissal) for inappropriate online conduct outside working time provided:
  - There is actual or potential damage to the education establishment's reputation.

- There is evidence of harassment/bullying. Discrimination or otherwise offensive behaviour.
- The education establishment has a clear policy making it clear what is acceptable and unacceptable; and
- The education establishment responds in a reasonable and proportionate way.

• You should seek advice from your HR Provider if you are considering disciplinary action.

Appendix 2 contains a draft policy for education establishments for their employees.

5. Guidance to Education establishment Staff

All education establishment staff should consider the following:

- Consider carefully what you post on your online profile so that you do not compromise your professional position.
- Ensure that your privacy settings are set correctly on the highest security level.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your education establishment, where you are currently employed/or have previously been employed at.
- Consider carefully before giving access to colleagues – are they really 'friends'?
- Do not make disparaging remarks about your education establishment/colleagues/pupils or any member of the education community. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Other users could post a photo on their profile where you could be named, so think about any photos you appear in. On Facebook, there is a tagging function you can enable onto your profile, which means everything you are tagged in i.e. pictures, comments, status' the function allows you to accept the content before it appears on your online profile and before it is connected to your name. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.
- It is recommended that members of staff do not to use their first name and surname on social media sites.
- Parents and pupils may access your online profile and could, if they find the information or images offensive, complain to your education establishment.
- Do not publish your date of birth and home address on any online profile. Identity theft is a crime on the rise with criminals using such information to access your bank or credit card account.
- Be aware of what monitoring, if any, maybe carried out by your education establishment.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.
- Make sure the GPS/ check-in facilities are disabled on the social networks you use. For example, Facebook uses GPS to geographically locate you in a status; this sometimes disables privacy settings and could allow students/parents to know your home address or where you are going for example places you visit/eating out.

6. Guidance on inappropriate online behaviour by parents/pupils/Governors

Online conduct by parents, pupils and Governors can have a devastating impact on individual teachers/staff and an education establishment. It has the potential to lead to stress related illness and absence from work. The education establishment should support any staff member when it becomes aware of any concerns. All employers have a duty of care to protect the health and safety of staff in the course of employment.

Key points:

- Ensure staff are aware they should let the education establishment (Headteacher) know of any concerns.
- Consider initially speaking to the child/parent/Governor and requesting they remove the post.
- Consider if criminal offences may have occurred and speak to your local police officer (see guidance in section 7 on legal issues).
- Report your concern to the host of the site in writing and ask that they remove the post.
- Most social media sites do have a report abuse button.

Appendix 4 contains a draft note to all parents if there are concerns and a specific letter to a parent when the education establishment has been made aware of a posting.

Photographs online

A related concern is the publishing of photographs by parents or education establishments online.

Education Establishment Photography.

Most education establishments now ask parents to indicate whether they consent to their children's photograph appearing online on the education establishment's website etc. A parental consent should be clear about the reason and purpose for any photographs taken. Parental consent will also be required if the education establishment records a play so that it can sell the recordings to. Any photograph should not allow an unauthorised person to identify a child or their whereabouts, so, if using a full name have no photograph, if using a photograph have no full name. Children in vulnerable circumstances like being in care or victims of parental violence should not be photographed at all unless there is clear consent and no risk.

For further information please see link below:
http://doncasterscb.proceduresonline.com/chapters/p_photo_young.html#use_image

Parents Photography

Concern remains over parents photographing their children at education establishment events.

- The Information Commissioner, who is responsible for overseeing data protection, has made it clear that images taken by parents for personal or recreational purposes such as with mobile phone, digital camera or camcorder are exempt from the Data Protection Act.
- However a education establishment may still have a policy restricting the taking of photographs or video or other images for child protection reasons or to prevent disturbances or because of concerns that parents have been using photos inappropriately.
- If you do allow photographs you may consider it appropriate to remind parents in writing and/or at the event that the photographs should only be for personal use and must not be posted on social media sites if they include other children. You may consider it appropriate on reply slips allocating tickets to ask parents to agree that any photographs taken must be used responsibly. You may also consider it appropriate to restrict photographs to the end of the event so that particular children can be removed from the photographs. It may also be appropriate for your education establishment to have a policy including a statement of parental responsibility for responsible use of images.
- There are a number of issues to consider with regard to this and the solution will be different for each education establishment. Your approach will depend on the particular issues and past concerns. You may wish to seek further advice if you have particular concerns.

Further information can be found at:

http://doncasterscb.proceduresonline.com/chapters/p_photo_young.html

7. Social Media – Basic Legal Issues

7.1 Copyright

- Copyright arises automatically in any original written or artistic work – there is no test of quality. It arises with posts, tweets, profiles, blogs and photos.
- Copyright in works created by an employee in the course of their duties belong to an employer.
- Copyright in works created by a student are owned by the student unless assigned to the education establishment (i.e. copyright policy).
- If copyright is infringed and the post was made by an employee in the course of employment, the employer may be liable.
- Each social media site has clear terms and conditions about what is published usually making it clear that by publishing a free license is given for it to be reproduced and made available to the rest of the world by anyone.

7.2 Law with regard to inappropriate posts

Civil offences

Defamation:

A false statement must be made negligently and publically resulting in damage.

It is considered that public bodies cannot bring defamation actions though individuals can (whether a public body can support their employee in doing this with financial backing is also questionable).

It is an expensive process in money and time and prevention is the best way – getting the comments removed by the individual or the Internet service provider (ISP).

Protection from Harassment Act 1997:

This provides a civil offence of harassment allowing an individual to obtain an injunction to stop harassment and to obtain damages as appropriate. Harassment is defined as a course of conduct (of at least 2 occasions) causing the victim alarm or distress.

Criminal offences

Malicious Communications Act 1998: This relates to a post that is 'grossly offensive'.

Recent Criminal Prosecution Service (CPS) guidance provides limited circumstances when they will consider prosecuting for a malicious communication, including where it amounts to credible threats of violence to the person or damage to property or harassment under the 1997 Act.

Protection from Harassment Act 1997: This act also provides for a criminal offence in addition to the civil offence mentioned above.

Sexual Offences Act 2003: This Act is often used by the police relating to grooming and other actions with children on social media.

8. Guidance with regard to Governors

It should be made clear to Governors the responsibility they have with their role, even though they are volunteers and unpaid they still have a high degree of responsibility.

In particular:

- Governors should not disclose information, make commitments or engage in activities on behalf of the education establishment, unless they are authorised to do so. This authority may already be delegated or may be explicitly granted depending on their role.
- Governors should not use social networking sites irresponsibly and ensure that neither their personal/professional reputation nor the education establishment's reputation is compromised by inappropriate postings.

Any such postings could lead to either suspension or removal from the Governing Body. Governors are asked to sign a Social Networking Agreement which has previously been made available to education establishments.

All Governors are expected to sign up to the Governors Code of Conduct on application/appointment. A copy of this Code can be found at http://www.doncaster.gov.uk/sections/educationandlearning/pupilandparentinformation/schoolgovernors/informationforschoolgovernors/Policies_and_Guidance_for_School_Governors.aspx

Governors are also expected to sign a declaration form as part of the appointment process which confirms that they will adhere to the Code of Conduct and not use social networking sites irresponsibly.

All Governors should consider the following;

- Consider carefully what you post on your online profile so that you do not compromise your professional position.
- Ensure that privacy settings are set correctly on the highest security level.
- Do not under any circumstances accept friend requests from a person you believe to be either a parent or a pupil at your education establishment, where you are currently a Governor/or have previously been a Governor.
- Consider carefully before giving access to colleagues – are they really 'friends'?
- Do not make disparaging remarks about your education establishment/colleagues/pupils or any member of the education community. Doing this in the presence of others may be deemed as bullying and/or harassment.
- Other users could post a photo on their profile where you could be named, so think about any photos you appear in. On Facebook, there is a tagging function you can enable onto your profile, which means everything you are tagged in i.e. pictures, comments, and statuses allows you to accept the content before it appears on your online profile and before it is connected to your name. If you do find inappropriate references to you and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.

- Parents and pupils may access your online profile and could, if they find the information or images offensive, complain to the education establishment.
- Do not publish your date of birth and home address on any online profile. Identity theft is a crime on the rise with criminals using such information to access your bank or credit card account.
- Be aware of what monitoring, if any, maybe carried out by the education establishment.
- Ensure that any comments and/or images could not be deemed defamatory or in breach of copyright legislation.

The Council has drafted a Social Networking Agreement which can be found at Appendix 5. It is advised that every new Governor is asked to sign it, and that it is reviewed annually.

9. Guidance for children

The Local Authority provides help and assistance to education establishments to develop education around safe and responsible behaviour online. Internet and technologies are a part of everyday life for our children and young people; and as we can't be with them to watch their every click, it is imperative that safeguarding and education in this area is embedded thoroughly. This guidance should be introduced to pupils at the beginning of each year.

eSafety is reviewed under behaviour and safety in school by OFSTED. The OFSTED inspection states that schools need to:-

- 'audit the training needs of all staff and provide training to improve their knowledge of and expertise in the safe and appropriate use of new technologies
- work closely with all families to help them ensure that their children use new technologies safely and responsibly both at home and at education establishments
- use pupils' and families' views more often to develop e-safety strategies
- manage the transition from locked down systems to more managed systems to help pupils understand how to manage risk, to provide them with richer learning experiences and to bridge the gap between systems at the education establishment and the more open systems outside the education establishment
- provide an age-related, comprehensive curriculum for e-safety that enables pupils to become safe and responsible users of new technologies
- work with their partners and other providers to ensure that pupils who receive part of their education away from the education establishment are e-safe
- Systematically review and develop their e-safety procedures, including training, to ensure that they have a positive impact on pupil's knowledge and understanding.

  For further information please see link below:
  http://www.ofsted.gov.uk/resources/briefings-and-information-for-use-during-inspections-of-maintained-schools-and-academies

- It should be made clear to pupils that having an online profile is against all rules and regulations in place if you access or create an account under the age of 13. This applies to Facebook, Twitter, Instagram, Snapchat and You Tube. (Please view rules for various other social networks).
- When accessing these accounts despite the rules in place pupils need to be aware of the amount of personal information they can potentially give away. General guidance around what is safe and what isn't should be talked about in the education establishment. For example an interest is ok; naming the education establishment they attend is giving away too much information.
- Pupils should be encouraged not to put pictures of them online but to use avatars or a picture of an interest e.g. a football. Pupils can give away information in images they upload especially in education establishment uniforms or any other uniform indicating a club they attend.
- Education around putting privacy settings on is imperative.
- Pupils should be made aware of the dangers GPS/ check-in facilities can potentially put them in. GPS and check in facilities allow pupils to

geographically locate themselves in a status. It can also identify their address and/or whether they are on holiday. If pupils were to use it when they are out visiting/eating with friends they could also be putting each other in danger. It is also advised that pupils do not check-in at school as this locates and posts what school they go to. GPS/check-in can come become automatic when it is enabled on smartphones.

- Pupils should be encouraged to be wary about publishing specific and detailed private thoughts online.
- Pupils are taught to consider their digital footprint.
- eSafety advice, updates and information should be given to pupils on a regular and meaningful basis.
- eSafety rules should be up around the education establishment so that children can see them; it is also advisable to have eSafety rules in the education establishment planners.
- Pupils should be made aware of how they can seek help and advice when problems online do occur, it is advised that the CEOP (Child Exploitation and Online Protection Centre) button is talked about in the education establishment and ideally embedded onto the education establishment website so that pupils are aware of where to go to if they needed to use it.
- Pupils need to be made aware of legislation which could affect what they put/do online particularly the Data Protection Act 1998. Staff should make them aware of this in an age appropriate manner.
- Parents should be contacted if it is highlighted that a child is accessing a site that is deemed to be inappropriate or not age appropriate.
- All new pupils need to be made aware of the rules and regulations around eSafety.
- All Students need to be made aware of whom the Designated Safeguarding Teacher/eSafety Officer is in the education establishment to discuss any concerns or worries.

Appendices

Appendix 1

Example Education establishment Social Media and Acceptable Use Policy for Students

Introduction

EDUCATION ESTABLISHMENT NAME recognises that access to technology in the education establishment gives students and teachers greater opportunities to learn, engage, communicate, and develop skills that will prepare them for work and life. We are committed to helping students develop 21st-century technology and communication skills.

This Acceptable Use Policy outlines the guidelines and behaviours that users are expected to follow when using education establishment technologies.

- The network is intended for educational purposes only.
- All activity over the network or using district technologies is monitored. Misuse of education establishment resources can result in disciplinary action.
- Students are expected to follow the same rules for good behaviour and respectful conduct online as offline.
- Users of the network or other technologies are expected to alert IT staff immediately of any concerns for safety or security.

Your ICT contact in the education establishment is _____

Technologies Covered

EDUCATION ESTABLISHMENT NAME may provide Internet access, desktop computers, mobile computers or devices, videoconferencing capabilities, online collaboration capabilities, message boards, email, and more.

As new technologies emerge, EDUCATION ESTABLISHMENT NAME will attempt to provide access to them. The policies outlined in this document are intended to cover all available technologies, not just those specifically listed.

Web Access

EDUCATION ESTABLISHMENT NAME provides its users with access to the Internet, including web sites, resources, content, and online tools. That access will be restricted in compliance with the education establishment's policies. Web browsing may be monitored and web activity records may be retained indefinitely.

Users are expected to respect that the web filter is a safety precaution, and should not try to circumvent it when browsing the Web. If a site is blocked and a user believes it shouldn't be, the user should follow protocol to alert an IT staff member or submit the site for review.

Email

EDUCATION ESTABLISHMENT NAME may provide users with email accounts for the purpose of education establishment-related communication. If users are provided with email accounts, they should be used with care. Users should not send personal information; should not attempt to open files or follow links from unknown or untrusted origin; should use appropriate language; and should only communicate with other people as allowed. Email usage may be monitored and archived.

Social / Web 2.0 / Collaborative Content
Recognising that collaboration is essential to education, EDUCATION ESTABLISHMENT NAME may provide users with access to web sites or tools that allow communication, collaboration, sharing, and messaging among users.
Users are expected to communicate with the same appropriate, safe, mindful, courteous conduct online as offline. Posts, chats, sharing, and messaging may be monitored. Users should be careful not to share personally-identifying information online.

Mobile Devices Policy
EDUCATION ESTABLISHMENT NAME may provide users with mobile computers or other devices to promote learning both inside and outside of the classroom. Users should abide by the same acceptable use policies when using education establishment devices off the education establishment network as on the education establishment network.
Users are expected to treat these devices with extreme care and caution; these are expensive devices that the education establishment is entrusting to your care. Users should report any loss, damage, or malfunction to IT staff immediately.

Security
Users are expected to take reasonable safeguards against the transmission of security threats over the education establishment network. This includes not opening or distributing infected files or programs and not opening files or programs of unknown or untrusted origin. If you believe a computer or mobile device you are using might be infected with a virus, please alert IT. Do not attempt to remove the virus yourself or download any programs to help remove the virus.

Plagiarism
- Users should not plagiarise (or use as their own, without citing the original creator) content, including words or images, from the Internet.
- Users should not take credit for things they didn't create themselves, or misrepresent themselves as an author or creator of something found online. Research conducted via the Internet should be appropriately cited, giving credit to the original author.

Personal Safety
If you see a message, comment, image, or anything else online that makes you concerned for your personal safety, bring it to the attention of an adult (teacher or staff if you're at an education establishment; parent if you're using the device at home) immediately.
- Users should never share personal information, including phone numbers, address, education establishment name, birthdays any other private information online.
- To ensure your safety, avoid talking about personal schedules or situations.
- Users should recognise that communicating over the Internet brings associated risks, and should carefully safeguard the personal information of themselves and others.
- Users should never agree to meet someone they meet online in real life.
- Users should also remember not to post anything online that they wouldn't want parents, teachers, or future colleges or employers to see. Once something is

online, it's out there - and can sometimes be shared and spread in ways you never intended.

Cyberbullying

- Cyberbullying is bullying through the internet and will not be tolerated. Harassing, dissing, flaming, denigrating, impersonating, outing, tricking, excluding, and cyberstalking are all examples of cyberbullying. Don't send emails or post comments with the intent of scaring, hurting, or intimidating someone else.
- Engaging in these behaviours, or any online activities intended to harm (physically or emotionally) another person, can always be tracked down by CEOP. Cyberbullying can be a crime. Remember that your activities are monitored and retained.

Examples of Acceptable Use

I will:

- Use education establishment technologies for education establishment-related activities and research.
- Follow the same guidelines for respectful, responsible behaviour online that I am expected to follow offline.
- Treat education establishment resources carefully, and alert staff if there is any problem with their operation.
- Encourage positive, constructive discussion if allowed to use communicative or collaborative technologies.
- Alert a teacher or other staff member if I see threatening/bullying, inappropriate, or harmful content (images, messages, posts) online.
- Use education establishment technologies at appropriate times, in approved places, for educational pursuits only.
- Be cautious to protect the safety of myself and others.
- Help to protect the security of education establishment resources.

This is not intended to be an exhaustive list. Users should use their own good judgment when using education establishment technologies.

Examples of Unacceptable Use

I will not:

- Use education establishment technologies in a way that could be personally or physically harmful to myself or others.
- Search inappropriate images or content.
- Engage in cyberbullying, harassment or disrespectful conduct toward others - staff or students
- Try to find ways to circumvent the education establishment's safety measures and filtering tools.
- Use education establishment technologies to send spam or chain mail.
- Plagiarise content I find online.
- Post personally-identifying information about myself or others.
- Agree to meet someone I meet online in real life.
- Use language online that would be unacceptable in the classroom.
- Use education establishment technologies for illegal activities or to pursue information on such activities.
- Attempt to hack or access sites, servers, accounts or content that isn't intended for my use.

This is not intended to be an exhaustive list. Users should use their own good judgment when using education establishment technologies.

Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges in extreme cases
- Notification to parents in most cases
- Detention or suspension from education establishment and education establishment-related activities
- Legal action and/or prosecution

I have read and understood this Acceptable Use Policy and agree to abide by it:

_____

(Student Printed Name)

_____

(Student Signature and date)

_____

I have read and discussed this Acceptable Use Policy with my child and have a full understanding of social media acceptable usage

_____

(Parent Printed Name)

_____

(Parent Signature and date)

_____

Appendix 2a)

Guidance on Using Social Media Responsibly

We encourage teachers, students (age depending), staff, and other education community members to use social networking/media (Twitter, Facebook, etc) as a way to connect with others, share educational resources, create and curate educational content. While social networking is fun and valuable, there are some risks you should keep in mind when using these tools. In the social media world, the lines are blurred between what is public or private, personal or professional.
We've created these social networking/media guidelines for you to follow when representing the education establishment in the virtual world.
Please do the following:

Use good judgment
- Regardless of your privacy settings, assume that all of the information you have shared on your social network is public information.

Be respectful
- Always treat others in a respectful, positive and considerate manner.

Be responsible and ethical when using social media as a communications tool
- Even though you are approved to represent the education establishment, unless you are specifically authorised to speak on behalf of the education establishment as a spokesperson, you should state that the views expressed in your postings are your own. Stick with discussing education establishment-related matters that are within your area of responsibility.

Be a good listener
- Keep in mind that one of the biggest benefits of social media is that it gives others another way to talk to you, ask questions directly and to share feedback but be careful it isn't used as a complaints service.
- Be responsive, provide answers, thank people for their comments, and ask for further feedback, etc.

Confidential information/ private and personal information
- Do not publish post or release information that is considered confidential or not public. Online conversations are never private. Do not use your birth date, address, place of work, phone number or any other private information online.
- To ensure your safety, avoid talking about personal schedules or situations.
- Never give out or transmit personal information about anyone else this includes all students, parents, or colleagues. Always respect the privacy of others.
- Don't take information you may receive through social networking (such as e-mail addresses, names or telephone numbers) and assume it's the most up-to-date or correct.

Images
- Respect brand, trademark, copyright information and/or images of the education establishment (if applicable).
- It is not acceptable to post pictures of students without the expressed written consent of their parents. It is also advised that pictures of students online do not have names connected to images.

- Any images containing information for example education establishment uniforms should be blurred out.
- Do not post pictures of colleagues or other members of the education community without their permission.

Other sites

- A significant part of the interaction on blogs, Twitter, Facebook and other social networks involves passing on interesting content or linking to helpful resources. However, the education establishment is ultimately responsible for any content that is shared. Don't carelessly repost a link without looking at the content first.
- Pay attention to the security warnings they're there to protect you and the education establishment.
- When using social networks, be sure to read and follow their printed terms and conditions.
- Be sure to correct any mistake you make immediately

Appendix 2b)

Guidance on Using Facebook Responsibly

Our education establishment is committed to promoting the safe and responsible use of the Internet and student's access to social media sites can be a concern. Whilst children cannot access Facebook or other social networking sites at the education establishment, they could have access to it on any other computer or mobile technology. Websites such as Facebook offer good communication and social connections, however they are created with their audience in mind and this is specifically 13 years old. Possible risks for children under 13 using the site may include:

- Facebook use 'age targeted' advertising and therefore your child could be exposed to adverts of a sexual or other inappropriate nature, depending on the age they stated they were when they registered.
- Children may accept 'friend requests' from people they don't know in real life which could increase the risk of inappropriate contact or behaviour (grooming).
- Language, games, groups and content posted or shared on Facebook is not moderated, and therefore can be offensive, illegal or unsuitable for children.
- Photographs shared by users are not moderated and therefore children could be exposed to inappropriate images or even post their own.
- Underage users might be less likely to keep their identities private and lying about their age can expose them to further risks regarding privacy settings and other options.
- Facebook could be exploited by bullies and for other inappropriate contact.
- Facebook cannot and does not verify its members therefore it is important to remember that if your child can lie about who they are online, so can anyone else.

We feel that it is important to point out to parents/carers the risks of underage use of such sites, so you can make an informed decision as to whether to allow your child to have a profile or not. These profiles will have been created away from the education establishment and sometimes by a child, their friends, siblings or even parents. We will take action (such as reporting aged profiles) if a problem comes to our attention that involves the safety or wellbeing of any of our children. Should you decide to allow your children to have a Facebook profile we strongly advise you to do the following:

- Check their profile is set to private and that only 'friends' can see information that is posted;
- Make sure they have privacy settings on to a high standard so they have to accept 'tags' in posts and pictures.
- Remove the location setting on statuses, this can pin point to their friends exactly what road they're stood on when writing something on Facebook.
- Monitor your child's use and talk to them about safe and appropriate online behaviour such as not sharing personal information and not posting offensive messages or photos;
- Ask them to install the CEOP (Child Exploitation and Online Protection Centre) application from www.facebook.com/clickceop on their profile. This places a

bookmark on their profile to CEOP and the 'Report Abuse' button which has been known to deter offenders;

- Have a look at the advice for parents/carers from Facebook www.facebook.com/help/?safety=parents
- Set up your own profile so you understand how the site works and ask them to add you as a friend on their profile so you can keep track of what they are posting online;
- Make sure your child understands the following rules:

  - Always keep your profile private;
  - Never accept friends you don't know in real life;
  - Never post anything which could reveal your identity;
  - Never post anything you wouldn't want your parents to see;
  - Never agree to meet someone you only know online without telling a trusted adult;
  - Always tell someone if you feel threatened or someone upsets you.

We recommend that all parents/carers visit the CEOP ThinkuKnow website for more information on keeping your child safe online or to report online abuse please see link below:

http://ceop.police.uk/safety-centre/

Appendix 3

Social Media Policy for Education establishment Employees

Social Media Policy For Bessacarr Primary School Staff

PERSON RESPONSIBLE FOR POLICY:	**(ADD NAME(S) HERE)**
APPROVED:	**DATE:**
SIGNED:	**ROLE:**
TO BE REVIEWED:	**(ADD DATE HERE)**

CONTENTS **PAGE**

1 INTRODUCTION

1.1 The internet provides a range of social media tools that allow users to interact with one another, for example from rediscovering friends on social networking sites such as *Facebook* to keeping up with other people's lives on *Twitter* and maintaining pages on internet encyclopaedias such as *Wikipedia*.

1.2 While recognising the benefits of these media for new opportunities for communication, this policy sets out the principles that Bessacarr Primary School staff and contractors are expected to follow when using social media.

1.3 It is crucial that pupils, their family members and the public at large have confidence in the education establishment's decisions and services. The principles set out in this policy are designed to ensure that staff members use social media responsibly so that confidentiality of pupils and other staff and the reputation of Bessacarr Primary School and Doncaster Council are safeguarded.

1.4 Staff members must be conscious at all times of the need to keep their personal and professional lives separate.

2 SCOPE

2.1 This policy applies to Bessacarr Primary School all teaching and other staff, whether employed by the Council or employed directly by the education establishment, external contractors providing services on behalf of the education establishment or the Council, teacher trainees and other trainees, volunteers and other individuals who work for or provide services on behalf of the education establishment. These individuals are collectively referred to as 'staff members' in this policy.

2.2 This policy covers personal use of social media as well as the use of social media for official education establishment purposes; including sites hosted and maintained on behalf of the education establishment (see sections 5, 6, 7 and Appendices A and B).

2.3 This policy applies to personal webspace such as social networking sites (for example *Facebook*, Twitter), blogs, mircoblogs, chatrooms, forums, podcasts, open access online encyclopaedias such as *Wikipedia,* social bookmarking sites such as *del.icio.us* and content sharing sites such as *flickr* and *YouTube*. The internet is a fast moving technology and it is impossible to cover all circumstances or emerging media - the principles set out in this policy must be followed irrespective of the medium.

3 LEGAL FRAMEWORK

3.1 Bessacarr Primary School is committed to ensuring that all staff members provide confidential services that meet the highest standards. All individuals working on behalf of the education establishment are bound by a legal duty of confidence and other laws to protect the confidential information they have access to during the course of their work. Disclosure of confidential information on social media is likely to be a breach of a number of laws and professional codes of conduct, including:

- the Human Rights Act 1998
- Common law duty of confidentiality, and
- the Data Protection Act 1998.

3.2 Confidential information includes, but is not limited to:

- Person-identifiable information, e.g. pupil and employee records and details protected by the Data Protection Act 1998
- Information divulged in the expectation of confidentiality
- Education establishment or Council business or corporate records containing organisationally or publicly sensitive information
- Any commercially sensitive information such as information relating to commercial proposals or current negotiations, or personal details for staff, pupils or their family members and
- Politically sensitive information.

3.3 Staff members should also be aware that other laws relating to libel, defamation, harassment and copyright may apply to information posted on social media, including:

- Libel Act 1843
- Defamation Acts 1952 and 1996
- Protection from Harassment Act 1997
- Criminal Justice and Public Order Act 1994
- Malicious Communications Act 1998
- Communications Act 2003, and
- Copyright, Designs and Patents Act 1988 and any updated laws.

3.4 Bessacarr Primary School could be held vicariously responsible for acts of their employees in the course of their employment. For example, staff members who harass co-workers online or who engage in cyberbullying or discrimination on the grounds of race, sex, disability, etc or who defame a third party while at work may render Bessacarr Primary School liable to the injured party.

4 RELATED POLICIES

4.1 This policy should be read in conjunction with the following education establishment and Council policies:

- Add relevant policies
- Reference to the council should be used where the education establishment is a maintained one or if some staff are employed directly by the Council.

5 PRINCIPLES – *BE PROFESSIONAL, RESPONSIBLE AND RESPECTFUL*

5.1 You must be conscious at all times of the need to keep your personal and professional lives separate. You should not put yourself in a position where there is a conflict between your work for the education establishment or Council and your personal interests.

5.2 You must not engage in activities involving social media which might bring Bessacarr Primary School or the Council into disrepute.

5.3 You must not represent your personal views as those of Bessacarr Primary School or the Council on any social medium.

5.4 You must not discuss personal information about pupils, their family members; Bessacarr Primary School or Council staff and other professionals you interact with as part of your job on social media.

5.5 You must not use social media and the internet in any way to attack, insult, abuse or defame pupils, their family members, colleagues, other professionals, other organisations, Bessacarr Primary School or the Council. You should ensure that at all times that you are not offensive, obscene, and discriminatory or harass others.

5.6 You must be accurate, fair and transparent when creating or altering online sources of information on behalf of Bessacarr Primary School or the Council.

5.7 You should ensure that you do not misuse confidential, sensitive or copyrighted information.

6 PERSONAL USE OF SOCIAL MEDIA

6.1 Staff should be aware that social network sites are not private and anything published on them is considered in the public domain. Your personal use of social media is not considered to be totally outside of the work domain and depending on your actions you may face disciplinary action at work for your personal use of social media.

6.2 Staff members must not identify themselves as employees of Bessacarr Primary School or Council or service providers for the education establishment or Council in their personal webspace. This is to prevent information on these sites from being linked with the education establishment and the Council and to safeguard the privacy of staff members, particularly those involved in providing sensitive frontline services.

6.3 Staff members must not have contact through any personal social medium with any pupil, whether from Bessacarr Primary School or any other education establishment, unless the pupils are family members. Staff members must decline 'friend requests' from pupils they receive in their personal social media accounts. If Staff Members receive such requests from pupils who are not family members, they must discuss these in general terms in class and signpost pupils to become 'friends' of the official education establishment site.

6.4 Bessacarr Primary School does not expect staff members to discontinue contact with their family members via personal social media once the education establishment starts providing services for them. However, any information staff members obtain in the course of their employment must not be used for personal gain nor be passed on to others who may use it in such a way.

6.5 Staff members must not have any contact with pupils' family members through personal social media if that contact is likely to constitute a conflict of interest or call into question their objectivity.

6.6 If staff members wish to communicate with pupils through social media sites or to enable pupils to keep in touch with one another, they can only do so with the approval of the education establishment and through official education establishment sites created according to the requirements specified in section 7 and Appendix A.

6.7 On leaving Bessacarr Primary School service; staff members must not contact Bessacarr Primary School pupils by means of personal social media sites. Similarly, staff members must not contact pupils from their former education establishments by means of personal social media.

6.8 Information staff members have access to as part of their employment, including personal information about pupils and their family members, colleagues Council staff and other parties and education establishment or Council corporate information must not be discussed on their personal webspace.

6.9 Photographs, videos or any other types of image of pupils and their families or images depicting staff members wearing education establishment or Council uniforms or clothing with education establishment or Council logos or images identifying sensitive education establishment or Council premises (eg care homes, secure units) must not be published on personal webspace.

6.10 Education establishment or Council email addresses and other official contact details must not be used for setting up personal social media accounts or to communicate through such media.

6.11 Staff members must not edit open access online material including but not limited to online encyclopaedias 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.

6.12 Bessacarr Primary School or Council corporate, service or team logos or brands must not be used or published on personal webspace

6.13 Bessacarr Primary School only permits limited personal use of social media while at work. Access to social media sites for personal reasons is not allowed between 9am and 5pm. There is a daily quota of 30 minutes to access these sites outside these hours. However, staff members are expected to devote their contracted hours of work to their professional duties and, in practice, personal use of the internet should not be on the education establishment's time. **NOTE: the education establishment must amend this statement in line with its own policy.**

6.14 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.

6.15 Staff members are strongly advised to ensure that they set the privacy levels of their personal sites as strictly as they can and to opt out of public listings on social networking sites to protect their own privacy. Staff members should keep their passwords confidential, change them often and be careful about what is posted online; it is not safe to reveal home addresses, telephone numbers and other personal information. It is a good idea to use a separate email address just for social networking so that any other contact details are not given away.

7 USING SOCIAL MEDIA ON BEHALF OF insert education establishment name

(This will only be relevant to secondary education establishments).

7.1 Staff members can only use official education establishment sites for communicating with pupils or to enable pupils to communicate with one another.

7.2 There must be a strong pedagogical or business reason for creating official education establishment sites to communicate with pupils or others. Staff must not create sites for trivial reasons which could expose the education establishment to unwelcome publicity or cause reputational damage.

7.3 Official education establishment sites must be created only according to the requirements specified in Appendix A of this Policy. Sites created must not breach the terms and conditions of social media service providers, particularly with regard to minimum age requirements.

7.4 Staff members must at all times act in the best interests of children and young people when creating, participating in or contributing content to social media sites.

8 MONITORING OF INTERNET USE

8.1 Bessacarr Primary School monitors usage of its internet and email services without prior notification or authorisation from users.

8.2 Users of Bessacarr Primary School email and internet services should have no expectation of privacy in anything they create, store, send or receive using the education establishment's ICT system.

9 BREACHES OF THE POLICY

9.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Bessacarr Primary School or Council Disciplinary Policy and Procedure.

9.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Bessacarr Primary School or the Council or any illegal acts or acts that render Bessacarr Primary School or the Council liable to third parties may result in disciplinary action or dismissal.

9.3 Contracted providers of Bessacarr Primary School or Council services must inform the relevant education establishment or Council officer immediately of any breaches of this policy so that appropriate action can be taken to protect confidential information and limit the damage to the reputation of the education establishment and the Council. Any action against breaches should be according to the education establishment's internal disciplinary procedures.

APPENDIX A

Requirements for creating social media sites on behalf of Bessacarr Primary School

A.1 CREATION OF SITES

A.1.1 Staff members participating in social media for work purposes are expected to demonstrate the same high standards of behaviour as when using other media or giving public presentations on behalf of Bessacarr Primary School.

A.1.2 Prior to creating a site, careful consideration must be given to the purposes for using social media and whether the overall investment is likely to be worthwhile for achieving the proposed pedagogical outcome.

A.1.3 The proposed audience and level of interactive engagement with the site, for example whether pupils, education establishment staff or members of the public will be able to contribute content to the site, must be discussed with the education establishment's appropriate manager (Nicola Cosgrove).

A.1.4 Staff members must consider how much time and effort they are willing to commit to the proposed site. They should be aware that maintaining a site is not a one-off task, but involves a considerable time commitment.

A.1.5 The headteacher of relevant managers must take overall responsibility to ensure that enough resources are provided to keep the site refreshed and relevant. It is important that enough staff members are trained and are able to maintain and moderate a site in case of staff absences or turnover.

A.1.6 There must be a careful exit strategy and a clear plan from the outset about how long the site will last. It must not be neglected, creating a potential risk to the education establishment's brand and image.

A.1.7 Consideration must also be given to how the success of the site will be evaluated to assess whether the site has achieved the proposed objectives.

A.2 CHILDREN AND YOUNG PEOPLE

A.2.1 When creating social media sites for children and young people and communicating with them using such sites, staff members must at all times be conscious of their responsibilities; staff must always act in the best interests of children and young people.

A.2.2 When creating sites for children and young people, staff members must be alert to the risks to which young people can be exposed. Young people's technical knowledge may far exceed their social skills and awareness – they may post sensitive personal information about themselves, treat online 'friends' as real friends, be targets for 'grooming' or become victims of cyberbullying.

A.2.3 If children and young people disclose information or display behaviour or are exposed to information or behaviour on these sites that raises safeguarding or other

concerns, appropriate authorities must be informed immediately. Failure to do so could expose vulnerable young people to risk of harm.

A.2.4 Staff members must ensure that the sites they create or contribute to for work purposes conform to the *Good Practice Guidance for the Providers of Social Networking and Other User Interactive Services* (Home Office Task Force on Child Protection on the Internet, 2008)(as amended/updated)

A.2.5 Staff members must also ensure that the webspace they create on third party sites comply with the site owner's minimum age requirements (this is often set at 13 years). Staff members must also consider the ramifications and possibilities of children under the minimum age gaining access to the site.

A.2.6 Care must be taken to ensure that content is suitable for the target age group and contributors or 'friends' to the site are vetted.

A.2.7 Careful thought must be given to the profile of young people when considering creating sites for them. For example, the internet may not be the best medium to communicate with vulnerable young people (or indeed any age group) receiving confidential and sensitive services from the education establishment or the Council. It may not be possible to maintain confidentiality, particularly on third-party-hosted sites such as social networking sites, where privacy settings may not be strong enough to prevent breaches of confidentiality, however inadvertent. If in doubt, you must seek advice from your appropriate manager (insert name).

A.3 APPROVAL FOR CREATION OF OR PARTICIPATION IN WEBSPACE

A.3.1 Bessacarr Primary School social media sites can be created only by or on behalf of the education establishment. Site administrators and moderators must be Bessacarr Primary School employees or other authorised people.

A.3.2 Approval for creation of sites for work purposes, whether hosted by the education establishment or hosted by a third party such as a social networking site, must be obtained from the appropriate manager (Nicola Cosgrove).

A.3.3 Approval for participating, on behalf of Bessacarr Primary School, on sites created by third parties must be obtained from the appropriate manager (Nicola Cosgrove).

A.3.4 Content contributed to own or third-party hosted sites must be discussed with and approved by the appropriate manager (Nicola Cosgrove).

A.3.5 The education establishment's appropriate manager (Nicola Cosgrove), must be consulted about the purpose of the proposed site and its content. In addition, the appropriate manager (Nicola Cosgrove), approval must be obtained for the use of the education establishment logo and brand.

A.3.6 Staff must complete the Social Media Site Creation Approval Form (Appendix B) and forward it to the education establishment's appropriate manager (Nicola Cosgrove), before site creation.

A.3.7 Be aware that the content or site may attract media attention. All media enquiries must be forwarded to the appropriate manager (Nicola Cosgrove) immediately. Staff members must not communicate with the media without the advice or approval of the appropriate manager (Nicola Cosgrove).

A.4 CONTENT OF WEBSPACE

A.4.1 Bessacarr Primary School hosted sites must have clearly expressed and publicised policies. Third-party hosted sites used for work purposes must have policies that conform to the education establishment or Council standards of professional conduct and service.

A.4.2 Staff members must not disclose information, make commitments or engage in activities on behalf of Bessacarr Primary School or the Council without authorisation.

A.4.3 Information provided must be worthwhile and accurate; remember what is published on the site will reflect on the education establishment's or Council's image, reputation and services.

A.4.4 Stay within the law and be aware that child protection, privacy, data protection, libel, defamation, harassment and copyright law may apply to the content of social media.

A.4.5 Staff members must respect their audience and be sensitive in the tone of language used and when discussing topics that others may find controversial or objectionable.

A.4.6 Permission must be sought from the relevant people before citing or referencing their work or referencing service providers, partners or other agencies.

A.4.7 Bessacarr Primary School -hosted sites must always include the education establishment logo or brand to ensure transparency and confidence in the site. The logo should, where possible, link back to the relevant page on the education establishment website.

A.4.8 Staff members participating in Bessacarr Primary School -hosted or other approved sites must identify who they are. They must disclose their positions within the education establishment on these sites.

A.4.9 Staff members must never give out their personal information such as home contact details or home email addresses on these sites.

A.4.10 Personal opinions should not be expressed on official sites.

A.5 CONTRIBUTORS AND MODERATION OF CONTENT

A.5.1 Careful consideration must be given to the level of engagement of contributors – for example whether users will be able to add their own text or comments or upload images.

A.5.2 Sites created for and contributed to by pupils must have the strongest privacy settings to prevent breaches of confidentiality. Pupils and other participants in sites must not be able to be identified.

A.5.3 The content and postings in Bessacarr Primary School.

A.5.4 -hosted sites must be moderated. Moderation is the responsibility of the team that sets up or initiates the site.

A.5.5 The team must designate at least two approved Administrators whose role it is to review and moderate the content, including not posting or removal of comments which breach the education establishment's policies. It is important that there are

enough approved moderators to provide cover during leave and absences so that the site continues to be moderated.

A.5.6 For third-party-hosted sites such as social networking sites used for work purposes, the responsibility for protection and intervention lies first with the host site itself. However, different sites may have different models of intervention and it is ultimately the responsibility of the staff member creating the site to plan for and implement additional intervention, for example in the case of content raising child safeguarding concerns or comments likely to cause offence.

A.5.7 Behaviour likely to cause extreme offence, for example racist or homophobic insults, or likely to put a young person or adult at risk of harm must never be tolerated. Such comments must never be posted or removed immediately and appropriate authorities, for example the Police or Child Exploitation and Online Protection Centre (CEOP), informed in the case of illegal content or behaviour.

A.5.8 Individuals wishing to be 'friends' on a site must be checked carefully before they are approved. Their comments must be reviewed regularly and any that do not comply with the social network guidance must not be posted or removed. **NOTE: the education establishment must amend this statement in line with their own policy. The safer alternative for education establishments is not to allow any outsiders to become friends of the site and to limit the site to known people only, in the case of adults, those who have undergone appropriate security checks.**

A.5.9 Any proposal to use social media to advertise for contributors to sites must be approved by the Headteacher.

A.5.10 Approval must also be obtained from the appropriate manager (Nicola Cosgrove) to make an external organisation a 'friend' of the site.

APPENDIX B

Bessacarr Primary School

Social Media Site Creation Approval Form

Use of social media on behalf of Bessacarr Primary School must be approved prior to setting up sites.

Please complete this form and forward it to the education establishment's **appropriate manager (Nicola Cosgrove)**.

TEAM DETAILS	
Department	
Name of author of site	
Author's line manager	

PURPOSE OF SETTING UP SOCIAL MEDIA SITE **(please describe why you want to set up this site and the content of the site)**	
What are the aims you propose to achieve by setting up this site? What is the proposed content of the site?	

PROPOSED AUDIENCE OF THE SITE
Please tick all that apply.

- ☐ Pupils of Bessacarr Primary School (aged 3-11 years)
- ☐ Bessacarr Primary School staff
- ☐ Pupils' family members
- ☐ Pupils from other education establishments (provide names of education establishments)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

PROPOSED CONTRIBUTORS TO THE SITE
Please tick all that apply.

- ☐ Pupils of Bessacarr Primary School (aged 3-11 years)
- ☐ Bessacarr Primary School staff
- ☐ Pupils' family members
- ☐ Pupils from other education establishments (provide names of education establishments)
- ☐ External organisations
- ☐ Members of the public
- ☐ Others; please provide details

ADMINSTRATION OF THE SITE	
Names of administrators (the site must have at least 2 approved administrators)	
Names of moderators (the site must have at least 2 approved moderators)	
Who will vet external contributors?	
Who will host the site?	☐ Bessacarr Primary School ☐ Third party; please give host name
Proposed date of going live	
Proposed date for site closure	
How do you propose to advertise for external contributors?	
If contributors include children or adults with learning disabilities how do you propose to inform and obtain consent of parents or responsible adults?	
What security measures will you take to prevent unwanted or unsuitable individuals from contributing or becoming 'friends' of the site?	

APPROVAL

(approval from relevant people must be obtained before the site can be created. The relevant managers must read this form and complete the information below before final approval can be given by the headteacher).

Appropriate Manager (insert name) **I approve the aims and content of the proposed site and the use of education establishment brand and logo.**	Name	
	Signature	
	Date	
Headteacher	Name	
	Signature	
	Date	

Appendix 4

Letters to Parents

General letter to all parents on social media

The education establishment is aware that social media is a useful tool that parents use to communicate. However the education establishment is concerned that negative comments may be made in such postings against the education establishment. You must be aware that such postings are considered in law to be accessible to the general public and you are therefore subject to the laws of defamation, malicious communication and improper use of the communications network. Any offensive or false allegations against the education establishment or its employees will be notified to the Police. If you have concerns with any aspect of your child's education and learning you should contact the Headteacher.

Example letter to parent on social media post.

Dear

It has been brought to our attention that you have made inappropriate comments on your (Facebook) site against teachers/pupils/staff at this education establishment.

The education establishment will not tolerate personal verbal attacks on any of its teaching staff/pupils particularly were they are abusive and offensive. We request that you remove the comments immediately.

You should be aware that any comments made on social media websites are considered to be in the public domain and they are subject to various laws including the Malicious Communications Act 1998, libel laws and protection from harassment legislation.

Should there be any repeat of these unfounded and degrading comments we will seek legal advice.

If you do have concerns with your child's education and learning you should contact the education establishment to arrange to see the class teacher or Headteacher.

Appendix 5

Governing Body Document

DONCASTER GOVERNORS' SUPPORT SERVICE

SOCIAL NETWORKING AGREEMENT

INTRODUCTION
Social Networking allows users to interact with one another in a virtual world. It is an online service, platform, or site that focuses on building and reflecting of social networks or social relations with people.

A social network service consists of a group of people showing his/her social links. Most social network services are web based and provide means for users to interact over the internet, such as email and instant messaging. The main social networking site used is Facebook.

IT IS NOT ADVISABLE:-

- To refer to the education establishment that you are a Governor at/or refer to any individual associated with that particular education establishment in any way on a social networking site.

- To upload pictures of any individual without the consent of the individual/parent or guardian in the course of education establishment business. However to follow best practice this should be avoided in a professional and personal capacity.

- To become an on-line 'friend' with any pupils/student at the education establishment.

- To upload any inappropriate/offensive language, images or comments on social networking sites that may bring you and the education establishment in disrepute. You should not publish anything that you do not want to be publicly associated with.

Think before you post! If in doubt, don't post or contact amy.simister@doncaster.gov.uk for further guidance.

Name: _____ a Governor at

_____ (education establishment) agree to adhere to the above statements in my role as Governor and understand that if I were to undertake any of the unadvisable actions this may lead to disciplinary action from my education establishment in addition to damaging the image of myself and that of the education establishment.

Signed: _____

Print: _____

Date: _____

Appendix 6

Contact Details

Further information can be obtained from:

Child Protection - Amy Simister

01302 736098 / amy.simister@doncaster.gov.uk

Governors' Support - Wendy Heath

01302 737279 / wendy.heath@doncaster.gov.uk

Legal - Helen Potts or Helen Wilson

01302 734631 / helen.potts@doncaster.gov.uk / helen.wilson@doncaster.gov.uk

Education Safeguarding Manager - Sarah Stokoe

01302 736743 / sarah.stokoe@doncaster.gov.uk

LADO (Local Designated Officer for Safeguarding) – Jim Foy
01302 737748 / lado@doncaster.gov.uk