Doncaster
Metropolitan Borough Council

Guidance on Social Media Use for Education Establishments

Person Responsible For Policy:	**K. Formby**
Approved:	**March 2020**
Signed:	**Head teacher:** **Chair of Management** **Committee:**
To be reviewed:	**March 2022**

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.

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 is 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.

Main social network sites:

- Twitter
- Facebook
- YouTube
- Snapchat
- Instagram
- Tumblr
- Linkedin
- TikTok
- Reddit

2 Appendix 1a Maple Medical PRU – Pupil Acceptable Use Agreement.
Appendix 1b Maple Medical PRU – Staff/Visitor/Governor Acceptable Use Agreement

Appendix 3 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.

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. 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.
  - Controlled or limited use during school 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.
- Staff should be made aware of 'staff exposure' on sites like ratemyteacher.com and various homemade groups. Whereby anyone is able to express an opinion on that person and their capabilities within the profession. If staff are made aware that they are being exploited within these types websites then appropriate action must be taken to safeguard the member of staff. Support and help can be found more on the following link. http://www.saferinternet.org.uk/advice-and-resources/teachers-and-professionals

- 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.

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. Staff should seek advice if unsure how to do this.
- 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.
- Make sure you have somewhere within your profile that 'opinions and comments are my own and not that of my employer'.
- 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.
- Staff should consider disabling GPs/ check in facilities on social networks. 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 / Management Committee members

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/MC member 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.

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 an 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.

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.

Maple Medical PRU purchases filtering service via the LA

8 Guidance with regard to Management Committee members

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

In particular:

- Management Committee members 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.
- Management Committee members 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 Management Committee. Management Committee members are asked to sign a Social Networking Agreement which has previously been made available to education establishments.

All Management Committee members are expected to sign up to the Governors Code of Conduct on application/appointment. A copy of this Code can be found at on the DMBC website.

Management Committee members 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 Management Committee members 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 Management Committee member 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.

e-Safety 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.
- 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).
- The e-Safety representatives should keep up to date with the constant change within the social media world and provide an update each term around new websites or trends so that others are aware of the latest dangers.
- 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.
- E-Safety advice, updates and information should be given to pupils on a regular and meaningful basis.
- E-Safety rules should be up around the education establishment so that children can see them;
- 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 e-Safety.
- All Students need to be made aware of whom the Designated Safeguarding Teacher/e-Safety Officer is in the education establishment to discuss any concerns or worries.

Appendix 1a

Maple Medical PRU: Pupil Acceptable Use Agreement e-Safety Rules/Social Media

Using ICT equipment:

- I will only use ICT in school for school purposes and as directed by school staff
- I will not tell other people my ICT passwords.
- I will only open/delete my own files.
- I will make sure that all ICT contact with other children and adults is responsible, polite and sensible.
- I will be responsible for my behaviour when using ICT because I know that these rules are to keep me safe.
- I will not bring in cds / memory sticks etc. from home and try to use them on the school system.

Using the internet:

- I will not deliberately look for, save or send anything that could be unpleasant or nasty. If I accidentally find anything like this I will tell my teacher immediately.
- I know that my use of ICT can be checked and that my parent/ carer contacted if a member of school staff is concerned about my e-Safety.
- I will not complete and send forms without permission from my teacher.
- I will not give my full name, home address or phone number when completing forms, unless as part of a directed lesson.
- I will always treat others in a respectful, positive and considerate manner.
- I will avoid talking about personal information online.
- I will never give out personal information about anyone else.

Using e-mail:

- I will ask permission before checking any email.
- I will only use my class email address or my own school email address when emailing.
- I will not send emails or post comments with the intent of upsetting, scaring or intimidating someone else.
- I will only email people I know or who my teacher has approved, and I will not open attachments without the permission of a member of staff.
- I understand that email messages I send or receive may be read by other people.
- I will immediately report any unpleasant messages sent to me.
- I will not give out my own details such as my name, phone number or home address.
- I will not use email to arrange to meet someone outside school hours.

Using social media:

- The use of social media sites in school is not allowed
- 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.

I have read this Acceptable Use Agreement and have a full understanding of e-safety rules and social media usage:

Pupil Printed Name: _____

Pupil Signature: _____ _____ (Date)

Appendix 2a)

Guidance on Using Social Media Responsibly

We ask that staff and students use any social media in a professional manner such as facebook groups for subject leaders/ exams officers/ resources etc.

We've created these social networking/media guidelines for you to follow when representing the education establishment in the online 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

Maple Medical PRU 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/

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 Maple Medical PRU 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 the education establishment and the Local Authority 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 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 Maple Medical PRU 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
- GDPR.

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 Maple Medical PRU 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 Maple Medical PRU liable to the injured party.

4 RELATED POLICIES

4.1 This policy should be read in conjunction with the following school and LA policies:

- Staff Code of Conduct
- Governors Code of Conduct

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 Maple Medical PRU or the LA into disrepute.

5.3 You must not represent your personal views as those of Maple Medical PRU or the LA on any social medium.

5.4 You must not discuss personal information about pupils, their family members; Maple Medical PRU or LA 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, Maple Medical PRU 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 Maple Medical PRU or the LA.

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 Maple Medical PRU or service providers for the education establishment or LA 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 Maple Medical PRU 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 Maple Medical PRU 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 Maple Medical PRU's service; staff members must not contact Maple Medical PRU's 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 Maple Medical PRU or LA corporate, service or team logos or brands must not be used or published on personal webspace

6.13 Any use of social media must be in a professional manner.

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 MONITORING OF INTERNET USE

7.1 Maple Medical PRU monitors usage of its internet and email services without prior notification or authorisation from users.

7.2 Users of Maple Medical PRU 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.

8 BREACHES OF THE POLICY

8.1 Any breach of this policy may lead to disciplinary action being taken against the staff member/s involved in line with Maple Medical PRU or LA Disciplinary Policy and Procedure.

8.2 A breach of this policy leading to breaches of confidentiality, or defamation or damage to the reputation of Maple Medical PRU or the LA or any illegal acts or acts that render

Maple Medical PRU or the LA liable to third parties may result in disciplinary action or dismissal.

8.3 Contracted providers of Maple Medical PRU or LA 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 LA. Any action against breaches should be according to the education establishment's internal disciplinary procedures.

Appendix 1b

MAPLE MEDICAL PRU

Staff, Management Committee and Visitor ICT Acceptable Use Agreement

ICT and the related technologies such as email, the internet and mobile devices are an expected part of our daily working life in school. This agreement, along with Maple Medical PRU's staff policy on Social Media is designed to ensure that all staff are aware of their professional responsibilities when using any form of ICT. All staff are expected to sign this policy and adhere at all times to its contents. Any concerns or clarification should be discussed with K. Formby, school e-Safety coordinator.

- I will only use the school's email / Internet / Intranet / Learning Platform and any related technologies for professional purposes or for uses deemed 'reasonable' by the Head or Governing Body.
- I will comply with the ICT system security and not disclose any passwords provided to me by the school or other related authorities.
- I will ensure that all electronic communications with pupils and staff are compatible with my professional role.
- I will only use the approved, secure email system(s) for any school business.
- I will ensure that personal data (such as data held on SIMS) is kept secure and is used appropriately, whether in school, taken off the school premises or accessed remotely. Personal data can only be taken out of school or accessed remotely when authorised by the Head or Governing Body.
- I will not install any hardware or software without permission of the Network Manager.
- I will not browse, download, upload or distribute any material that could be considered offensive, illegal or discriminatory.
- Images of pupils and/ or staff will only be taken, stored and used for professional purposes inline with school policy and with written consent of the parent, carer or staff member. Images will not be distributed outside the school network without the permission of the parent/ carer, member of staff or Headteacher.
- I understand that all my use of the Internet and other related technologies can be monitored and logged and can be made available, on request, to the Headteacher.
- I will respect copyright and intellectual property rights.
- I will ensure that my online activity, both in school and outside school, will not bring my professional role into disrepute.
- I will support and promote the school's e-Safety policy and help pupils to be safe and responsible in their use of ICT and related technologies.

<u>School Equipment</u>

I accept that when school lap-tops, digital cameras etc. are taken home I must sign the appropriate form and adhere to the conditions specified.

User Signature

I agree to follow this code of conduct and to support the safe use of ICT throughout the school:

Signature …… Date …….

Full Name ……. (printed)

Job title . . . . . .

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 Management Committee member at

Maple Medical PRU, agree to adhere to the above statements in my role as MC member 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: _____

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