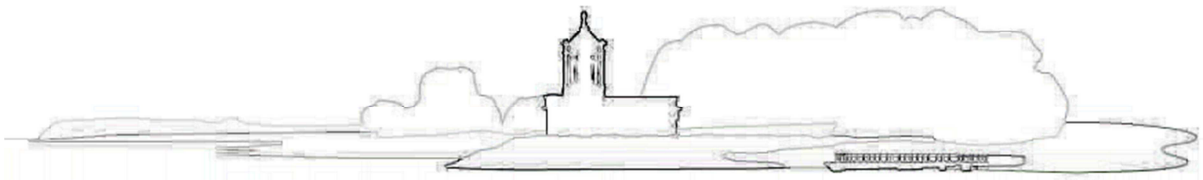
APPENDIX B

Rutland County Council

SOCIAL MEDIA POLICY

Version & Policy Number	Version 1
Guardian	Human Resources
Date Produced	January 2015
Next Review Date	January 2017

Approved by SMT	13 January 2015
Approved by LJC	18 June 2015
Approved by EAC	



Summary of document

The Social Media Policy describes the benefits and concerns relating to the use of social media sites. It identifies the responsibilities of employees who act on behalf of the Council, in the use of social media, both in a professional and personal capacity. It provides guidance regarding the access to and use of social media, and specifies the implications to the Council and individuals if social media is improperly used, whether this is inadvertent or deliberate.

Contents

1.0 Introduction

Rutland County Council is committed to making the best use of all available technology and innovation to improve the way we do business. This includes using all reasonable and cost-effective means to improve the way we communicate, reach out and interact with the different communities we serve.

'Social media' is the term commonly given to web-based tools which allow users to interact with each other in some way – by sharing information, opinions, knowledge and interests online. As the name implies, social media involves the building of online communities or networks to encourage participation and engagement.

These platforms open up many new and exciting opportunities. However, the practical application of such technology by the Council is continually developing and there are many potential issues to consider – both as individual employees and as a Council. Developments are regularly arising from legislation and case law, with conduct issues and the increase in cyberbullying and harassment regularly making headlines.

To avoid mistakes which could result in reputational, legal and ethical issues, and misuse/abuse of a well functioning social media relationship, it is important that we manage any potential risks through a common-sense approach and framework as well as proactively monitoring the development of such applications.

1.1 Aim and purpose of the Policy

The aim of this policy is to provide managers and employees with advice and guidance on their responsibilities concerning the use of, or the development of, any social media application, and to help them get the best from the tools available whilst maintaining a safe professional environment and protecting themselves, as well as the Council.

The purpose of this policy is to provide clear guidance about acceptable behaviour and the Council's expectations of employees regarding social media both at work and out of work, to ensure that:

- The Council is not exposed to legal or governance risks
- The reputation of the Council is not adversely affected or damaged by inappropriate use
- Social media is used appropriately by the Council as an additional communications channel when it is identified that its use will enhance engagement with specified target groups
- The public is able to distinguish clearly that where information is provided via social media that it is legitimately representative of the Council

The overarching principle behind this policy is that the standards that are expected for online conduct are, in essence, no different to offline conduct.

1.2 Definition of Social Media

For the purposes of this policy, social media is a type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes online social networking sites such as Twitter and Facebook. Social media also covers blogs and video- and image-sharing websites such as YouTube and Flickr.

Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly changing area. Employees should follow these guidelines in relation to any social media that they use.

1.3 Risks

Social media sites are a public forum and individuals should not assume that their entries on such sites will remain private. The Council must ensure that confidentiality, the rights of others connected with the Council, and the reputation of the Council itself are protected at all times. Additionally, the Council wishes to reduce the risk of employees contravening legislation and Council policies with respect to data protection, bullying and harassment, and discrimination, or falling foul of libel, defamation and copyright laws.

2.0 Scope

This policy is applicable to **all** employees of the Council and is recommended to those schools where the Governing Body performs the function of the employer.

The policy also applies to contractors, agency workers, volunteers, student/work experience placements or other partners or third parties working on behalf of the Council, collectively referred to as Council representatives throughout the remainder of this policy.

This policy applies to the use of social media for both business and personal purposes, whether during office hours or otherwise. It also applies whether the social media is accessed using Council IT facilities or equipment belonging to staff members.

This policy should be read in conjunction with Employee Code of Conduct, Grievance Policy and Procedure (which includes bullying, harassment and discrimination) and ICT Internet and E-Mail Policy.

3.0 Principles

3.1 Use of social media at work

3.1.1 Access to Social Media for Work Purposes

Council representatives should be aware that their relationship with social media changes as soon as they identify themselves as a Council representative, speak in any kind of professional capacity, or use social media on Council business. Individuals are the public face of the Council and should participate in the same way as they would with other media or public meetings or forums.

Participation online will result in comments being permanently available and open to being republished via other communication channels, e.g. they may attract media interest in the individual or the Council.

Details of all corporate social media accounts, and those who have access to these, are held by the Strategic Communications Advisor. Passwords should be changed when team members leave the Council to ensure the ongoing security of the access to the account, and the Strategic Communications Advisor informed accordingly.

3.1.2 Access via personal devices

Employees must not use their own equipment (e.g. smartphone) to access social media (eg. use of Facebook and Twitter) during their normal working hours. Usage should be restricted to breaks and time outside working hours.

Any employee currently using social media for Council business, and accessing it from a home computer, MUST get permission from their manager, inform the Strategic Communications Adviser of their activity and make sure they comply with the contents of this policy.

3.1.3 Guidelines on the Use of Social Media for Work Purposes

Council representatives must take the following into consideration when using social media in a professional capacity:

- **You are personally responsible for any content you publish**: Be mindful that it is in the public domain and on the record potentially permanently. Anything you publish will reflect directly on the Council as a whole.
- **Clearly identify yourself and your role:** Make it clear that you are acting in an official capacity on behalf of the Council.
- **Be professional**: Make sure you are always seen to act in an honest, accurate, fair and responsible way at all times. Always remember that you are an ambassador for the organisation.
- **Be aware of your association with the Council in all online spaces**: Ensure your profile and related content is consistent with how you wish to present yourself with colleagues and customers.
- **Be aware of your language and conduct**: The rules governing conduct such as the Council's Code of Conduct, Grievance Policy and Procedure and the Equal Opportunities policy still apply. Also, as in all publishing, you should be aware of issues such as libel, defamation and slander. Avoid 'textspeak', slang and any form of wording that may not be generally understood by everybody, unless you have a clear specific target audience.
- **Obtain approval from your Manager and inform the Strategic Communications Adviser** Ensure you have the full approval of your Manager, and seek advice from the Strategic Communications Adviser before any official use of social media. Always alert your Manager and the Strategic Communications Adviser early if you think you may have made a mistake. Councillors would be advised to similarly consult with the Strategic Communications Advisor and political lead.

- **Always stay within the legal framework**: Never share confidential or sensitive information and be aware that data protection and financial regulations apply.
- **Seek permission before publishing information that is not already in the public domain**: This includes documents, details of conversations, addresses etc. Do not cite or reference customers, partners or suppliers without their approval.
- **Respect copyright**: when linking to images or other online material. Seek appropriate advice on this to ensure accidental breaches are avoided.
- **Assess any risks**: Think through any potential risks and make sure you have plans in place to manage and mitigate these.
- **Do not post any personal information that may be used to identify you or colleagues**: this includes home addresses, personal contact details etc
- **Monitoring and evaluation**: Make sure you have a plan for how you intend to monitor and evaluate the success of your activity.

3.2 Use of social media in your personal life

Whilst it is acknowledged that when participating in social media for personal use, the views and opinions that individuals express are their own, it is important to be aware that posting information or views about the Council cannot be isolated from a person's professional working life.

Information published online can, if unprotected, be accessed around the world within seconds and can make them identifiable to service users as well as people they know in a private capacity.

The Council views any comment that is made on a social media site is made publicly and any inappropriate or offensive comments made will be considered in the context of which it is made. For example, disparaging comments about the Council, Members or colleagues made on the internet could be viewed as bullying/harassment, defamation or could be considered to bring the Council into disrepute. This may be deemed as a disciplinary offense.

Employees should be mindful that all comments made through social media must meet the standards of the Data Protection Act, Code of Conduct and the Equality and Diversity policy.

Employees should ensure that clients known to them through their work, where there could be a conflict of interest, are not linked to them through social media. The Council considers it inappropriate to have either current or former service users as "friends" through social media, especially where these people are vulnerable and there may be safeguarding issues. For example, it would be inappropriate for social workers to have service users and their families as friends on Facebook.

Online sites such as Facebook are in the public domain and personal profile details can be seen by anyone, even if users have their privacy settings on the highest level as these can be compromised by "friends" who have not set their security to the same standard.

If you have a LinkedIn profile then you must ensure that, whenever your profile relates to your employment by us:

- It is accurate,
- It does not divulge confidential or sensitive material, or material which might lower the reputation of the Council
- You refer to the Council and your employment in a way which is respectful

Individuals should be aware that they are personally responsible for any content they publish. If the comments published are contrary to any of the Council's policies, impacts on or compromises the employee's ability to undertake their role, or undermines management decisions, such behaviour could be considered a serious breach and be investigated and may result in disciplinary action being taken and ultimately could result in dismissal.

3.2.1 Guidelines on the Use of Social Media for Personal Use

Given that individuals are personally responsible for any content published the following should be taken into consideration:

- It is good practice to not mention work, your opinions of your colleagues or processes and projects on your own private Social Media Networks. Although you may believe you are sharing information with trusted friends, you need to recognise the risk of circulation outside this circle.
- Remember that commenting on or reposting messages will link you to the original statement, and could be viewed that you are condoning the opinions expressed
- Statements made on personal social media accounts will be assumed to have been made by that individual unless they can provide convincing evidence to the contrary
- Employees should be aware that the Employees' Code of Conduct covers the issues of fidelity and information disclosure, and should bear this in mind when using social media in a personal capacity outside of work.
- Employees should not engage in activities on the internet that might bring the Council, its Officers or Members into disrepute.
- Do not use Council branding, graphics (including Council photographs) or literature on personal social media pages.
- Do not reveal information which is confidential to the Council - consult your manager if you are unsure.
- Do not include contact details or photographs of service users or staff without their permission.
- Employees should be aware that any reports of inappropriate activity, linking them to the Council, will be investigated.
- With the rise in identity theft and fraud, employees may wish to consider the amount of personal information that they display on their personal profile.
- Use the Council's whistleblowing procedure to raise any issues of malpractice – this is the appropriate channel for raising issues in the first instance, not social media sites.
- Report to HR or IT if you see anything on a social media site that indicates that a colleague may have breached this policy.

4. Posting Responsible Content on Social Media Sites

In summary, any communications that employees make in a personal or professional capacity through social media must not:

- bring the Council into disrepute, for example by:
  - criticising or arguing with service users, colleagues or rivals;
  - making defamatory comments about individuals or other organisations or groups; or
  - posting images that are inappropriate or links to inappropriate content;
- breach confidentiality, for example by:
  - revealing confidential or sensitive information owned by the Council;
  - giving away confidential information about an individual (such as a colleague or service user contact)
  - discussing the Councils internal workings (such as future plans or proposals not yet made public)
- breach copyright, for example by:
  - using someone else's images or written content without permission; or
  - failing to give acknowledgement where permission has been given to reproduce something;
- do anything that could be considered discriminatory against, or bullying or harassment of, any individual, for example by:
  - making offensive or derogatory comments relating to sex, gender reassignment, race (including nationality), disability, sexual orientation, religion or belief or age;
  - using social media to bully another individual (such as another employee of the Council); or
  - posting images that are discriminatory or offensive or links to such content.

5. Use of social media in the recruitment process

As part of the recruitment process, the Council may make use of open-source information about applicants in order to protect service users and the Organisation. Whether or not this is required for a particular role will be considered on a case by case basis. If used, this would be undertaken as late in the process as reasonably practicable, and candidates notified of the intention to conduct this in advance of this taking place. If any information found gives cause for concern, this will be discussed with the potential candidates before any decisions are taken. Advice should be sought from Human Resources in all cases.

6. Monitoring

Rutland County Council reserves the right to monitor and access employees' internet usage, in line with the ICT Security Policy and Email and Internet Policy**.** The Council considers that valid reasons for checking an employee's internet usage include suspicions that the employee has:

- been using social media websites during working hours; or
- acted in a way that is in breach of the rules set out in this policy.

The Council reserves the right to retain information that it has gathered on employees' use of the internet in line with the systems monitoring outlined in the IT Security Policy, or for the duration of any 'live' disciplinary sanctions.

Access to particular social media websites for Council purposes may be withdrawn in any case of misuse.

7. Non-compliance

All employees are required to adhere to this policy. Employees should note that any breaches of this policy, whether as a result of deliberate or inadvertent misuse, may lead to disciplinary action. Serious breaches of this policy, for example incidents of bullying of colleagues or social media activity causing damage to the Council (for example bringing the Council's reputation into disrepute or exposing it to potential liabilities), may constitute gross misconduct and lead to summary dismissal. Other breaches may also be considered to be serious breaches, depending on the circumstances, and your role within the Council.

You must remove any material posted in breach of this policy upon our request.

You must co-operate to the fullest extent possible in any investigation into suspected breaches of this policy. This may include handing over any relevant passwords for equipment, accounts and in situations where we need these passwords in order to investigate a suspected breach.

8. Policy review

This policy will be kept up to date and amended accordingly to reflect any changes in response to this policy and applicable standards and guidelines.

A large print version of this document is available on request

Rutland
County Council

Rutland County Council
Catmose, Oakham, Rutland LE15 6HP

01572 722 577
enquiries@rutland.gov.uk
www.rutland.gov.uk