Acceptable Use of Social Media Policy

February 2019

Table of Contents

BOLTON COUNCIL

SOCIAL MEDIA POLICY

1. Introduction

Bolton Council recognises that the Internet provides a unique opportunity to participate in interactive discussions and share information using a wide variety of social media, such as Facebook, Twitter, Instagram, LinkedIn and blogs. Employees are likely to use social media in a private capacity outside of work and they may also be required to use it in a business capacity as part of their role at the Council.

However, employees' use of social media in both a personal and business capacity can present risks to our confidential information and reputation, and can jeopardise our compliance with legal obligations. To minimise these risks, and to ensure that our IT resources and communications systems are used appropriately, we expect employees to adhere to this policy.

The purpose of this policy is to assist employees by providing clear guidance about acceptable behaviour on social media both in work and out of work. It is consistent with the regulations and conditions of service which employees should already be aware of in their work for the Council.

Staff working with vulnerable groups should also be mindful of the information in the '' Guidance for Safer Working Practices for Adults Who Work With Children and Young People ''document and other relevant publications.

2. Scope

This policy applies to all employees of the Council and is recommended to those schools where the Governing Body performs the function of the employer. The policy is also recommended as a guide regarding social media use by Members and / their agents. Members should consider when using social media whether they are doing this in their role as a "Councillor'' or in a personal capacity. Members should keep in mind how what they post may be perceived and that issues can arise under The Council's Code of Conduct for Members when using social media.

This policy also applies to agency and casual workers, volunteers and those on apprenticeships and student/work experience placements, working on behalf of the Council. The term "employees" is used throughout but covers all these groups.

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

This policy should be read in conjunction with the Grievance Procedure and Anti-Harassment Policy Statement, The Council's Code Codes and Protocols for Members and Officers , ICT Acceptable Use Policy, Media Policy and Procedure and the RIPA Policy and Guidance October 2016.

3. Exclusions

The social media policy will not apply where there are other separate, specific Council procedures to address an issue, *e.g. whistleblowing policy.*

4. Relevant Legislation

The Human Rights Act 1998 gives a 'right to respect for private and family life, home and correspondence'. The provision is directly enforceable against public sector employers. Case law suggests that employees have a reasonable expectation of privacy in the workplace.

The Regulation of Investigatory Powers Act 2000 covers the extent to which organisations can monitor or record communications at the point at which they enter or are being sent within the employer's telecommunications system. It applies to public and private communication networks.

The Data Protection Act 2018 ("The DPA") and the General Data Protection Regulations ("GDPR") covers how information about people can be collected, handled and used.

5. Definitions

Social media is the term used for online tools, websites and interactive media that enable users to interact with each other by sharing information, opinions, knowledge and interests. This policy and guidelines cover social media issues over the internet and by email, smart phones, social networking sites, blogging, and tweeting that are directly work related or through personal use that can be directly or indirectly linked to work.

For the purposes of this policy the term 'social media' covers sites and applications including but not restricted to Twitter, Facebook, Flickr, YouTube, Snapchat ,Instagram, LinkedIn, blogs, discussion forums video and image sharing websites and wiki sites.

There are many more examples of social media than can be listed here and this is a constantly changing area. This policy refers to the examples listed ,and also any other existing or new social media which is developed in the future.

6. Personal Safety and Privacy

Employees need to be aware that the information they post on their personal social media profile can make them identifiable to service users, as well as people they know in a private capacity.

Employees should therefore consider this when setting up their online profile particularly in relation to; use of a photograph, providing details of their occupation, employer, and work location.

Employees should ensure that clients known to them through their work or *where there could be a conflict of interest* are not linked to them through social media. The Council considers it inappropriate to have 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 may be seen by anyone, even if users have restricted their privacy settings. Also if a user's profile is linked to other sites, any changes to their profile may also be updated there.

Employees who have set their privacy level to the maximum can have their privacy compromised by 'friends' who may not have set their security to the same standard.

Employees should remember that their online presence is not always controlled by them

7. Key Principles

7.1 Personal accountability and responsibility

All employees are expected to behave appropriately and responsibly, and should be aware that they may be accountable to the Council for actions outside of their work.

Online conduct is the employee's responsibility, and it is important that employees are aware that posting information on social networking sites in a personal capacity cannot be entirely isolated from their working life. Staff should consider that photos they post can have a reputational impact as can inappropriate comments that they make on line.

Any information published online can be accessed around the world within seconds and will be publicly available for all to see, and is not easy to delete/withdraw once published.

The Council's view is that any comment that is made on a social media site is made publicly, and that any inappropriate comment made, will be considered in the context of which it is made.

For example, disparaging comments against a colleague/other made on Facebook could be viewed as bullying/harassment, or could be considered to bring the Council into disrepute.

Employees are advised to be mindful that all comments made through social media must meet the standards of the Data Protection Act, GDPR**,** The Council's Code Codes and Protocols for Members and Officers and the Equality Policy Statement. You should also be mindful of the standards required by any professional body to which you belong.

Employees should if they receive contact via social media from a service user consider the need to report this to their manager as soon as is possible. Communication with service users/clients should be made only via official council systems.

Employees may be accountable for actions outside of work, including making comments on social media sites, if that is contrary to any of Council's policies, impacts on or compromises the employee's ability to undertake their role. Such behaviour could be investigated and may result in disciplinary action being taken, and ultimately could result in dismissal. Employees should refrain from making inappropriate comments on social media regarding colleagues or the Council.

Further employee guidance is available in the Appendix 1.

7.2 Access to social media for work purposes

Employees who use social media as part of their job must adhere to the Council's Media Policy and Procedure. Local authorities and therefore our employees are expected to comply with The Code of Recommended Practice on Local Authority Publicity (the 'Publicity Code') issued on the 31 March 2011.

Employees must be aware that they are representing the Council when they are contributing to the Council's social media activities. Employees should use the same safeguards as they would with any other form of communication about the organisation in the public domain.

Employees should be mindful that social media can be used by the online criminal community to deliver malware, malicious software such as a virus, and carry out schemes designed to damage property or steal confidential information.

Council social media accounts must not be used at any time for Party political purposes or political party campaigning.

Employees should also consider the honesty and reliability of what they publish.

When sharing photographs/copying information staff should be mindful that permissions may be required due to copyright and privacy laws.

When moderating any kind of online space that is managed by Bolton Council, there are house rules about what kind of content is acceptable. The Council agrees to publish all contributions from users (whether we agree with what the user is saying), providing that they do not break these rules.

If there is a supported business case for a member of staff having access to social media for work purposes they should contact Corporate ICT for approval. Requests are logged through the Agilisys support desk and need to be approved by a manager. All other Council staff should be blocked from accessing social media via Council IT. If you need to set up a new social media account please contact the web team on email@bolton.gov.uk or call 01204 331024.

Please find at Appendix 2 our House Rules for users who contribute to our social media sites.

7.3 Access to social media at work, for personal use

Employees should not access social media websites for personal use from the Council's computers or devices.

Leaving Social Media sites 'running' constantly in work time is considered to be a breach of the ICT Acceptable Use Policy.

7.4 Any communications that employees make through social media must not:

- **Bring the organisation into disrepute, for example by:**
  - Criticising, disagreeing or arguing with customers, colleagues or managers;
  - Making defamatory comments about individuals or other organisations/groups;
  - Posting images that are inappropriate or links to inappropriate content;

- **Breach confidentiality, for example by:**

- Referring to confidential information about an individual (such as a colleague or service user) or the Council

- **Breach people's rights where there is a reasonable expectation of privacy**

- **Do anything that could be considered discriminatory against, or bullying or harassment of, any individual or group of individuals, and in contravention of the Council's procedures, 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 an employee of the Council); or
  - Posting images that are discriminatory or offensive or links to such content.

- **Any other action that impacts on the employees ability to do their job, for example by:**
  - Online activity that is incompatible with the position they hold in the Council
  - Any breach occurring inside or outside the workplace that is likely to affect the employee doing his/her work.

- **Contravene the Council's policies, for example;**
  - The Council's Codes and Protocols For Members and Officers, Grievance Procedure, Anti- Harassment Policy Statement, Data Protection Policy, Information Security Policy or the Equality Policy Statement.

The above examples are not a definitive list of the misuse of social media, but are examples to illustrate what misuse may look like. Employees are encouraged to talk to their manager and seek advice if they are unclear.

8. Social Media and Confidentiality [Please read alongside the RIPA Policy and Guidance October 2016]

Increasingly local authorities are turning to the online world, especially social media, when conducting investigations. The Chief Commissioner's 2015 annual report at 5.42 stated that, "*just because this material is out in the open, does not render it fair game." The Surveillance Commissioners have provided guidance that certain activities will require authorisation under RIPA or RIP(S)A and this includes repetitive viewing of what are deemed to be "open source" sites for the purpose of intelligence gathering and data collation."* It should not be assumed by staff therefore that all monitoring of open social media sites are automatically immune from the need for an authorisation of some sort. Use of open media, in circumstances where there is a reasonable expectation of privacy, is likely to require an authorisation, particularly if the monitoring is intensive or for a prolonged period of time i.e. more than a week or so. Staff should seek legal advice

before monitoring social media sites to see whether the criteria for RIPA authorisation is met/some other authorisation process needs to be followed. The creation of fake or anonymous websites for investigation purposes is likely to require an authorisation. Entry on to chat rooms or closed groups for investigatory purposes is also likely to require authorisation and/advice from the Governance Team. Whilst overt working in this way might avert the need for a surveillance authorisation, officers should be aware that a CHIS [Covert Human Intelligence Source] situation could inadvertently arise.

It is expected that social media sites will generate significant amounts of sensitive information. Sensitive material that is not relevant to an investigation should be quickly and safely disposed of. Any interaction between an investigator and the public via social media could inadvertently give rise to a CHIS situation. Investigators should generally avoid interaction whilst monitoring social media sites and take advice should any uncertainty arise. The use of internet and social media may require an Authorisation in the following circumstances:

1. Any Communications which are made with 3rd parties for the purpose of gathering evidence or intelligence about an offence in circumstances where the third party is not aware that the officer is working for the Local Authority.

2. Accessing private pages of social media for the purpose of gathering evidence or intelligence about an offence or other matter subject to potential litigation.

3. Communication between an officer and a 3rd party for the purpose of using that person to gather evidence or intelligence about a suspect.

4. Intensive monitoring of a suspect using social media over a sustained period of time particularly when this is used in connection with other methods of investigation.

5. Creation of a false personae or use of a third parties identity for investigation purposes.

6. Any direct interaction in any forum – open or closed – in which an officer seeks to elicit information, if they are not explicit about their real identity.

Repeated entry to social media sites and copying material for the purpose of an investigation is likely to engage the need for an authorisation process to be followed.

As a rule of thumb access to Facebook and other social media sites should be made via the Council's Facebook account as opposed to a private account. If there is any doubt, the officer who is conducting this activity is advised to take legal advice.

The use of social media should be guided by the principles of public confidence, legitimacy, accountability , visible compliance with the rule of law, proportionality, minimal

intrusion, and engagement with the public.

9. Addressing allegations of misuse

All employees are required to adhere to this policy. Comments made through social media may constitute an act of misconduct or gross misconduct, which could lead to dismissal, if the comments contravene any of the Council's policies or if they lead to a breakdown in the relationship of mutual trust and confidence.

Managers should ensure that all complaints are dealt with consistently and fairly.

Breaches of this policy may be dealt with in line with the Dismissal and Disciplinary procedure. Serious breaches could result termination of the employment contract and where applicable, may result in civil action and/or criminal charges.

Further support/advice on these HR Policies can be sought from your manager in the first instance. Thereafter you could discuss the matter with your departmental HR section who may refer you to IT regarding technical issues.

Contacts are listed on the intranet here: HR contacts
http://portal.bolton.gov.uk/ChiefExecutives/PeopleandTransformation/HumanResources/Pages/HRContacts.aspx

10. Roles and responsibilities

Employees have a responsibility to:

- Avoid behaviour that may cause an individual to feel the subject of harassment or bullying.
- Familiarise themselves with the Social Media policy and employee Guidance to on the use of Social Media in the Appendix.
- Act responsibly when using online media for both work and personal use.
- Report instances to their manager, if they are subject to abuse, threats or harassment.
- Advise their manager if they believe there has been a breach of policy.

Managers have a responsibility to:

- Familiarise themselves with the Social Media policy and Guidance on the use of Social Media in the Appendix.
- Take prompt action to stop any harassment or bullying they become aware of, whether a complaint has been raised or not
- Ensure their staff are aware of the Social Media policy and employee guidelines

- Support employees who are the subject of abuse.
- Ensure all complaints/allegations are dealt with fairly and consistently, and in accordance with other policies and procedures where appropriate.
- Provide support to their staff using social media about impartiality, confidentiality, conflicts etc.

HR staff have a responsibility to:

- Provide support and advice to managers and employees on the operation of the policy and guidelines, where necessary.

11. Further Guidance

An Employees' Guide to the use of social media is attached in the Appendix 1.

This policy also works alongside other policies including the Internet and Email Acceptable Use Policy, Employee and Member Code of Conduct, Disciplinary Procedure and the Grievance Procedure and Anti–Harassment Policy Statement, copies of which are available on the intranet or from your manager.

The use of social media will also be embedded in the Council's emergency plan

APPENDIX 1

EMPLOYEE GUIDANCE ON THE USE OF SOCIAL MEDIA

- Employees must be mindful that any online activities/comments made in a public domain, must be compatible with their position within the Council, and safeguard themselves in a professional capacity.

- Employees are expected to be responsible users and to stay safe when using technology

- Employees should protect their own privacy and ensure that their social media accounts do not compromise their professional position.

- Comments made outside work, within the arena of social media, do not remain private and so can have an effect on or have work-related implications. Therefore, comments made through social media, which you may intend to be "private" may still be in contravention of The Council's Codes And Protocols For Members and Officers, the Grievance Procedure and Anti-Harassment Policy Statement and/or the Dismissal and Disciplinary Policy. Once something is online, it can be copied and redistributed making it easy to lose control of. Presume everything you post online will be permanent and can be shared.

- LinkedIn contacts are, at the time of writing this policy, considered by case law to belong to the employer where they are linked to an employee's work.

- Avoid exposing the Council to any reputational, brand or legal risks.

- Consider setting your privacy controls to their highest possible setting and keep in mind that your posts could be seen by friends of friends etc.,

- Do not set up fake pages to pose as others.

- Do not give your personal details to service users.

- Do not use your work e mail address for personal accounts.

- Do not post content that may be seen as racist, sexist, homophobic, bullying or threatening or otherwise inappropriate.

- Do not discuss work-related issues online, including conversations about service users, complaints, management or disparaging remarks about colleagues or the Council. Even when anonymised, these are likely to be inappropriate. In addition doing this in the presence of others may be deemed as bullying and/or harassment.

- Do not under any circumstances accept friend requests from a person you believe could be a service user or may conflict with your employment.

- Be aware that other users may access your profile and if they find the information and/or images it contains offensive, make a complaint about you to the Council as your employer.

- Do not use your work email for private social media accounts.

- Ensure that any comments and/or images cannot be deemed bullying, defamatory, libellous or in breach of copyright legislation.

- When setting up your profile online, consider whether it is appropriate and prudent for you to include a photograph, or provide occupation, employer or work location details.

- You can take action if you find yourself the target of complaints or abuse on social networking sites. Most sites will include mechanisms to report abusive activity and provide support for users who are subject to abuse by others.

- If you do find inappropriate references and/or images of you posted by a 'friend' online you should contact them and the site to have the material removed.

- If you are concerned about someone else's behaviour online, you should take steps to raise your concerns. If these are work related you should inform your manager.

- Employees should also act in accordance with the Council's Code of Conduct, ICT Acceptable Use Policy, Data Protection Policy, Information Security Policy, Grievance Procedure and Anti-Harassment Policy Statement.

- Employees must not use social media for monitoring/investigations without considering the need for an authorisation of some sort.

APPENDIX 2

Bolton Council: Digital engagement

We're happy to help you in any way that we can and look forward to seeing your views and feedback. We do however expect our users to offer us the same level of courtesy that we offer them, so we have a short set of house rules:

1. All users must comply with the social media platform's Terms of Use as well as these Terms of Use.

2. We will remove, in whole or in part, posts that we feel are inappropriate.

3. We will report and remove any social media profiles that are set up using bolton.gov.uk imagery, including fonts, without permission.

4. We will block and/or report users on Twitter who direct tweets at us which we believe are:

    a) Abusive or obscene
    b) Deceptive or misleading
    c) In violation of any intellectual property rights
    d) In violation of any law or regulation
    e) Spam (persistent negative and/or abusive tweeting in which the aim is to provoke a response)

5. You are wholly responsible for any content you post including content that you choose to share.

Anyone repeatedly engaging with us using content or language which falls into the above categories will be blocked and/or reported to the associated social media platform.

Responding to users:

1. We'll do our best to respond to your enquiries within four working hours.

2. We'll try to help you, or direct you to people and/or departments who can, wherever possible.

3. Our working hours are 9.00 – 17.00 Monday to Friday. We'll deal with enquiries sent outside of this time as soon as possible when working hours resume.

4. The @boltoncouncil twitter account is here to provide information and support for users of the bolton.gov.uk website.

5. The @boltoncouncil Twitter account is not a political account and cannot respond to political tweets.

We do not respond to tweets of a commercial nature

Whilst we are happy to receive such material, we will not respond as we are governed by strict procurement rules.

We reserve the right to modify or change these conditions at any time.

We look forward to hearing from you!