

<b>REPORT TO:</b>	<b>STANDARDS COMMITTEE</b>
<b>DATE:</b>	7 November 2017
<b>REPORT OF:</b>	Sandra Stewart – Borough Solicitor (Monitoring Officer)
<b>SUBJECT MATTER:</b>	<b>SOCIAL MEDIA USE: RESPONSIBLE CONDUCT POLICY</b>
<b>REPORT SUMMARY:</b>	To consider the Social Media Use Responsible Conduct Policy which has been refreshed and updated to take on board learning and best practice since the policy was last approved as part of the Information Governance Framework which was presented to the Standards Committee in October 2013.
<b>RECOMMENDATION(S)</b>	The Committee are asked to comment and recommend that this policy be adopted by the Council.
<b>FINANCIAL IMPLICATIONS:</b> (Authorised by Borough Treasurer)	There are no significant financial issues arising from this Report.
<b>LEGAL IMPLICATIONS:</b> (Authorised by Borough Solicitor)	It is important that employees are fully advised of what is expected of them in a clear and accessible way.
<b>RISK MANAGEMENT:</b>	Standards Committees should be aware of the National position in order that consistency of approach is taken in respect of setting and advising on local ethical and standard issues.
<b>LINKS TO COMMUNITY PLAN:</b>	Support the current arrangements for ethical and corporate governance of the Council to ensure that the public can have confidence in the ability of the Standards Committee.


**ACCESS TO INFORMATION**

**NON-CONFIDENTIAL**

**This report does not contain information which warrants its consideration in the absence of the Press or members of the public**

**REFERENCE DOCUMENTS:**

The background papers relating to this report can be inspected by contacting the report writer, Wendy Poole, the Head of Risk Management and Audit Services.

 Telephone: 0161 342 3846

 e-mail: [wendy.poole@tameside.gov.uk](mailto:wendy.poole@tameside.gov.uk)

# **Social Media Use: Responsible Conduct Policy**

---

**November 2017**

## **SOCIAL MEDIA USE: RESPONSIBLE CONDUCT POLICY**

**(This policy covers all employees, agency workers and consultants representing the Council.**

### **CONDUCT**

As an organisation, we encourage communication among our employees, residents, customers, partners, and others - and Web logs (blogs), social networks, discussion forums, wikis, video, and other social media - such as Twitter - can be a great way to stimulate conversation and discussion. They are also an invaluable tool to share information and consult.

The Internet provides a number of benefits in which Tameside council employees may wish to participate. From rediscovering old school friends on *Facebook* to keeping up with other people's daily lives on *Twitter* or helping to maintain open access online encyclopaedias such as *Wikipedia*. Even if your social media activities take place completely outside of work, as your personal activities should, what you say can have an influence on your ability to conduct your job responsibilities, your work colleagues' abilities to do their jobs, and Tameside's business interests.

Accordingly, where an employee is clearly identifiable as being an employee of the Council and/or discusses their work, they are expected to behave appropriately when on the Internet, and in ways that are consistent with the Council's values and policies. This guidance note sets out the principles which Council employees are expected to follow when using the Internet and gives interpretations for current forms of interactivity. It applies to blogs, to microblogs like *Twitter* and to other personal web space. The Internet is a fast moving technology and it is impossible to cover all circumstances. However, the principles set out in this document should always be followed.

The intention of this guidance is not to stop Council employees from conducting legitimate activities on the Internet, but serves to flag-up those areas in which conflicts can arise.

Tameside Council's reputation for impartiality, objectivity and fairness is crucial. The public must be able to trust the integrity of Tameside councillors, employees and its services. Our residents and partners audiences need to be confident that the outside/private activities of our employees do not undermine the Council's reputation and that its actions are not perceived to be influenced by any commercial or personal interests.

To this end employees/agency workers and consultants:

- Should NOT engage in activities on the Internet which might bring the Council into disrepute;
- Should NOT conduct themselves in a way that is detrimental to the Council;
- Should NOT use the Internet in any way to send or post abusive, offensive, hateful or defamatory messages, especially those which concern members of the public, councillors, customers/service users, employees, agency staff, consultants or the Council;
- Should Not 'like' a comment of this nature;
- Should NOT post derogatory or offensive comments on the Internet;
- Should NOT act in a way which could reputationally damage the council;
- Should NOT act in a way that damages the Council's or the public's trust and confidence in an employee's fitness to undertake their role;
- Should act in a transparent manner when altering online sources of information;
- Should NOT post information that could constitute a breach of copyright or data protection legislation;
- Employees (including agency workers and consultants should only use their work email addresses for official Council business;

- Should NOT use the Council's ICT Systems for party political purposes or for the promotion of personal financial interests; and
- Should take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees (including agency workers and consultants) and the public.

Individuals in politically restricted posts (usually over salary scale point 44), those that provide regular advice and support to committees and panels or speak with the press and those that work in politically sensitive areas should not be seen to support any political party or cause. Any online activities associated with work for the Council should be discussed and approved in advance by a senior council manager.

All employees (including agency workers and consultants) should be mindful of the information they disclose on social networking sites. Where they associate themselves with the Council (through providing work details or joining a council employee network) they should act in a manner which does not bring the Council into disrepute. Employees (including agency workers and consultants) need to be mindful that even though they do not associate themselves with the Council, others on the social networking site may be able to identify them and make the association.

Employees will be aware that use of the internet at work is provided primarily for business use. However the Council recognises that many employees use the internet for personal purposes and that many employees participate in social networking on websites such as Facebook, Twitter, Myspace, Bebo and Friendster (this list being for illustrative purposes only). Alongside such social networking sites the internet also offers employees the opportunity to access and post on blogs, twitter, wikis and other online forums.

The purpose of this guidance is to outline the responsibilities of employees using social networking websites and other online forums. It forms part of the Council's existing Information Governance Framework and the Councils Employee Code of Conduct.

### **Personal use of the internet at work**

The Council has devoted time and effort into developing the ICT Systems to assist you with your work. The Council does, however, recognise that there are times when you may want to use the ICT Systems for non-work related purposes, and in recognising this need the Council permits you to use the ICT Systems for responsible personal use.

You must not use the ICT Systems for personal use during working hours. If you work flexible hours then personal use must be at a time when you are not working and outside core time. You must not allow personal use of the ICT Systems to interfere with your day- to-day duties or of others.

If you choose to use the Council's ICT Systems to access social networking sites and/or other online forums, blogs etc. you must do so in a responsible and appropriate manner. There is no unconditional right for an Employee to access such sites and the Council reserves the right to restrict access to the internet (or certain websites) for particular employees if there is cause for concern over their use.

Employees should be aware that social networking websites are a public forum, particularly if the employee is part of a "network". Employees should not assume that their entries on any website will remain private.

### **Personal conduct whilst in work or outside the workplace**

The Council respects an employee's right to a private life. However, the Council must also ensure that confidentiality and its reputation are protected.

Employees are reminded of the unique way in which information posted on the internet can be quickly disseminated and control over such information can be rapidly lost. As such, employees should think about what information they are posting and how this could reflect on them and the Council especially in light of the difficulty they may encounter in trying to remove such information. Where comments are removed there is no guarantee that removing the source comment removes it from all websites.

Employees (including agency workers and consultants) using social networking websites and/or online forums outside of work are requested to:

- Refrain from commenting on any aspect of the Council's business, on any Council policy issue or issues at work. Adding a disclaimer that the views are your own and not those of the Council, will not protect you from potential disciplinary action should concerns be raised or reported;
- Ensure that they do not conduct themselves in a way that is detrimental to the Council;
- Never send or post abusive, offensive, hateful or defamatory messages about members of the public, councillors, other employees (including agency workers and consultants, customers, service users or the Council); and
- Take care not to allow interaction on these websites that could cause damage to working relationships between councillors, employees (including agency workers and consultants, customers, service users and/or members of the public.

### **Monitoring of online access at work**

You should note that, in order to protect its legitimate business interests and its ICT Systems, the Council monitors internet use in accordance with the provisions set down in the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy, and unacceptable levels of use could lead to disciplinary action.

### **Inappropriate Posting**

If an employee is found to have posted inappropriate material in any format on the internet, they are required to assist in any way to ensure such material is removed without delay. Failure to assist in removing such material in a timely fashion could lead to disciplinary action being taken against that employee.

### **Disciplinary Implications**

If the Council finds that an employees' internet use is not in accordance with the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy or this guidance, access to the internet may be withdrawn.

Employees are reminded they should never send or post inappropriate, abusive or defamatory messages on the internet either whilst in work or outside the workplace. Any messages which are abusive, offensive or defamatory could cause damage to the council's reputation and distress and anxiety to others in the workplace and employees are reminded of their obligations under the Council's Code of Conduct, Equalities Policy and Data Protection Policy.

Employees must be aware that if such matters do come to light, disciplinary action may be taken in line with the Council's Disciplinary Procedure if deemed sufficiently serious, this could result in dismissal.

### **Security and identity theft**

Employees are reminded to be security conscious and take steps to protect themselves from identity theft, for example by restricting the amount of personal information that they give out. Social networking websites and online forums allow people to post detailed personal information

such as date of birth, place of birth and favourite football team, which can form the basis of security questions and passwords.

Employees must take care when posting such information, in order that it does not allow a breach of security within the Council, or raise the possibility of the employee's identity being stolen.

In addition, employees should:

- Ensure no information is made available that could provide a person with unauthorised access to the Council and/or any confidential information belonging to the Council, councillors, other employees and/or members of the public; and
- Refrain from recording any confidential information regarding the Council, councillors other employees and/or members of the public on any social networking website.

## WHAT IS SOCIAL MEDIA?

Facebook, Twitter, blogs, YouTube, Wikipedia and networking sites such as LinkedIn are all examples of social media. The term covers anything on the internet where content is created and adapted by the people who use the site and which allows two-way conversations.

The Tameside **Social media use: responsible conduct policy** applies to:

- All blogs, wikis, forums, and social networks hosted or sponsored by Tameside;
- Your personal blogs that contain postings about Tameside's business, councillors, employees, residents, customers, or partners;
- Your postings about Tameside's business, councillors, employees, residents, customers, or partners, on any external blogs, wikis, discussion forums, or social networking sites such as Twitter; and
- Your participation in any video related to Tameside's business, councillors, employees, residents, customers, or partners; whether you create a video to post or link to on your blog, you contribute content for a video, or you appear in a video created either by another Tameside employee or by a third party.

## WHY DO LOCAL COUNCILS NEED SOCIAL MEDIA?

Local authorities and other public sector agencies are increasingly looking to social media to engage with their audiences for two broad reasons:

1. **The audience is changing** - People also expect to 'talk back' when official bodies communicate with them and they expect that those agencies will in turn respond and do so in appropriate language. New media enables that kind of interaction to happen in a more efficient manner than, for instance, arranging regular public meetings. Also our audience is becoming fragmented and diverse in so many ways. The traditional ways of communicating where budget is invested into a newsletter or another form of mass communication that contains one standard message and assumes this will be effective for everybody is increasingly losing impact. Information needs to be provided in a variety of formats so each target audience can choose how to access it. Photographs can tell a thousand words and videos are very accessible for a wide audience.
2. **Pressure from Central Government** - We all know that public funds are being squeezed from the centre as the focus becomes much tighter on how money is spent, especially on communications. **There** is also an ethos in some areas of Whitehall that e-government needs to be incentivised and **encouraged**. For these reasons, central government is looking more closely at the degree to which local authorities are using new media to talk to their audiences and this is becoming an increasing factor in the awarding of funds/grants.

## **WHAT ARE THE BENEFITS OF USING SOCIAL MEDIA?**

Used carefully, social media can bring people together over common interests; can be useful for consulting people and getting feedback and publishing information that other media may ignore. However, you must treat social media with respect. Always remember any information or comments you publish on any site (internal or external):

- May stay public for a long time;
- Can be republished on other websites;
- Can be copied, used and amended by others;
- Could be changed to mis-represent what you said; and
- Can attract comments and interest from other people/the media.

Always be aware of the standards, conditions of use and guidelines for posting laid down by the owner of any site or network and make sure you comply with them.

## **USING SOCIAL MEDIA**

This policy applies to you participating in any on-line social media (whether listed here or not), whether privately or as part of your role with the Council and sets out the standards of behaviour the Council expects of all its employees.

You are permitted to use social media from a Council computer at work, provided you comply with the Council's Email, Communications and Internet Acceptable Use Policy and this guidance, and ensure that you use it in a reasonable manner, unless you are specifically using it to undertake Council business e.g. consultation with the public, that you only engage in such social interaction in your own time.

You must make sure any on-line activity does not interfere with your job, your colleagues, your responsibilities and duties as a Council employee, our commitment to customers, is legal and does not bring the Council into disrepute. If you are found to be in breach of any of these policies, then you may face disciplinary action.

## **STAY LEGAL**

You must stay within the law at all times. Be aware that fair use, financial disclosure, libel, defamation, copyright and data protection laws apply on-line just as in any other media. Remember that colleagues and customers may see your online information (e.g. Facebook). Whether you identify yourself as an employee of Tameside Council or not, think carefully about how much personal information you want to make public and make sure your profile and the information you post reflects how you want them to see you both personally and professionally.

Never give out personal details like home addresses, phone numbers, financial information or full date of birth to prevent identity theft.

In addition, a person that posts grossly offensive or indecent matter may be found guilty of an offence under the Communications Act 2003 and could be sentenced to up to 6 months imprisonment and/or be fined up to £5,000.

## **KEEP IT PRIVATE AND DECENT**

**Remember your obligations** to residents, service users, partners, suppliers and colleagues and to protecting the Council's reputation. Never give out details of or divulge dealings with colleagues, customers or partners without their explicit consent. Check with your manager if you are not sure

what is and isn't confidential.

**Never make offensive comments** about any customer, supplier, partner or any of their employees or your Council colleagues. Don't use ethnic slurs, personal insults, obscenity or behave in ways that would not be acceptable in the workplace. That could bring the Council into disrepute, break the law and leave you open to prosecution and/or disciplinary action.

**Don't pick fights**, be the first to correct your mistakes and don't alter previous posts without indicating that you have done so.

**Don't be afraid to be yourself**, but be considerate about other people's views, especially around 'controversial' topics such as politics and religion. You can challenge without being abusive.

**Be credible, be accurate, fair and thorough** and make sure you are doing the right thing.

**Share useful information** that you gain from using social media with others, where appropriate.

**Speaking for the Council**, you should not 'speak for the Council' (disclose information, publish information, make commitments or engage in activities on behalf of the Council) unless you are specifically authorised to do so in writing. If you have not been authorised, then please speak to your line manager and the Council's communications team before taking any action.

**Remember** you are personally liable for what you publish online.

If you are unsure please contact your line senior council manager in the first instance or:

- Sarah Dobson – Assistant Director Policy, Performance and Communications
- Sandra Stewart – Director – Governance and Pensions (Borough Solicitor/Monitoring Officer)
- Aileen Johnson – Head of Legal Services

## **GIVING YOUR PERSONAL VIEWS**

1. Be professional, responsible and honest and try to add value to any debate. Remember that if people know your **links** with the Council you will be seen as representing the whole Council (even if you are not speaking on our behalf) so be careful.
2. If you are discussing or publishing any information on a website about the Council or council/work related matters, you must make it clear that you are speaking for yourself and not on behalf of Tameside Council. The easiest way to do this is to write in the 'first person' (I think, my view is.) and use a disclaimer, however, this will not protect you from potential disciplinary action should concerns be raised or reported.
4. Be aware that you may attract media interest in you as an individual, so be careful whenever you use social media for personal or business reasons. If you have any doubt, speak to your line manager and the Council's Communications Team before you go on-line.
5. If the media do contact you about something posted on-line, politely ask for their contact details, say you will get back to them and take advice from the Council's Communications Team before any response is given.

## **GUIDELINES FOR BLOGGING/BLOGGERS**

1. Please see the "Keep it private and decent" section
2. If you already have a personal blog or website which shows in any way that you work at Tameside Borough Council you must tell your manager. You should include a simple and visible disclaimer such as "The views expressed here are my own and don't necessarily represent the views of Tameside Borough Council"



3. If you want to start blogging, and your blog/website will say that you work for Tameside Council you should tell your manager and use the disclaimer.
4. If you think something on your blog or website may cause a conflict of interest or have concerns about impartiality or confidentiality, speak to your manager. If in any doubt, don't talk about what you do at work – particularly if you work in sensitive areas (such as social work) or on high profile, controversial projects. The Council has to be seen as honest, transparent, fair and impartial at all times. You must not undermine that.
5. If someone offers to pay you for blogging this could cause a conflict of interest and you must inform your manager.

## **GUIDELINES FOR SOCIAL NETWORKS, DISCUSSION FORUMS, WIKIS ETC**

1. Please see the "Keep it private and decent" section
2. Use your best judgment. Remember that there are always consequences to what you publish.
3. Don't use your work email account or your email or work number in on-line discussions unless you have been authorised to speak for the Council.
4. It is not a good idea to invite customers to become your friends on social networking sites. There may be a conflict of interest, security and privacy issues
5. Make sure any wiki entries, articles or comments are neutral in tone, factual and truthful.
6. Never post rude or offensive comments on any online encyclopaedias
7. Before editing an online encyclopaedia entry about the Council, or any entry which might cause a conflict of interest or adding links, check the house rules of the site. You may also need permission from the relevant wiki editor and your line manager.
8. If you edit online encyclopaedias whilst using a work computer, the source of the correction may be recorded as a Tameside Borough Council IP address. That means it may look as if the Council itself has made the changes. If this is correcting an error about the Council, that's fine – we should be open about our actions. In other circumstances be careful that you do not bring the Council into disrepute through this. If in any doubt, ask the Council's communications team before taking action.
9. We should respond to legitimate criticism with facts but please speak to the Council's communications team for advice before responding; a poor response could make matters worse. Never remove criticism of the Council or derogatory or offensive comments. Report them to the site administrator for them to take action.

## **GUIDELINES FOR 'MEDIA' SHARING (VIDEO, PHOTOS, PRESENTATIONS)**

1. Make sure all video and media is safe to share, does not contain any confidential or derogatory information, and is not protected by any copyright or intellectual property rights.
2. If the content is official Tameside Council content then it must be labelled and tagged as such.
3. Individual work must be labelled and tagged as such. Use a disclaimer where appropriate: "This is my personal work and does not necessarily reflect the views of Tameside Borough Council." Please note that a disclaimer will not protect you from potential disciplinary action should concerns be raised or reported.

## **USE OF COUNCIL COMPUTER EQUIPMENT**

1. Make sure you have read, understood and signed the Council's ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy. This sets out very clearly what you can and cannot do.
2. You must protect the security of our network and information at all times.
3. Do not install any application.
4. Do not open emails from people you don't know and trust, particularly if they have attachments. Do not forward these within the council unless you know they are virus free.
5. Remember online activity can be traced back to the Council and you. Don't do anything online

that breaches the ICT Security Policy and the Email, Communications and Internet Acceptable Use Policy and this guidance.

6. Do not reveal any details of the Council's ICT systems and services, including what software we use for email, internet access and virus protection to minimise the risk of malicious attack.
7. If you use secure systems, such as GovConnect email or to process financial transactions, never log onto social networking sites while connected to those systems. If you have used a social networking site, please restart your computer before logging onto the secure system to clear any information in the computer's memory cache.

## **LEGAL ISSUES**

### **Libel**

If you publish an untrue statement about a person which is damaging to their reputation they may take a libel action against you. This will also apply if you allow someone else to publish something libellous on your website if you know about it and don't take prompt action to remove it. A successful libel claim against you will result in an award of damages against you.

### **Copyright**

Placing images or text from a copyrighted source (e.g. extracts from publications, photos etc.) without permission is likely to breach copyright. Avoid publishing anything you are unsure about or seek permission in advance. Breach of copyright may result in an award of damages against you.

### **Data Protection**

Avoid publishing the personal data of individuals unless you have their express written permission.

### **Bias and Pre-determination**

If you are involved in planning or licensing application or other quasi-judicial decisions, avoid publishing anything that might suggest you don't have an open mind about a matter you may be involved in determining. If not, the decision runs the risk of being invalidated.

### **Obscene material**

It goes without saying that you should avoid publishing anything that people would consider obscene. Publication of obscene material is a criminal offence.

## **GUIDELINES FOR MANAGERS**

Please make sure you and your employees (including agency workers and contractors) are aware of and working within these guidelines. Please speak to the Assistant Director of Policy, Performance and Communications, Legal, ICT or Human Resources if you have any questions or concerns about interpreting this policy.

Managers are responsible for deciding what is appropriate, bearing in mind concerns about impartiality, confidentiality, conflicts of interest or commercial sensitivity.

If you believe any employee is breaching these guidelines or is spending too much time on the internet/social media), ask ICT to activate internet monitoring for that employee. It is your responsibility as a manager to ensure your employees (including agency workers and consultants) are not abusing Council ICT facilities.

## **FINALLY....**

These guidelines are to protect you and the reputation of the Council. They are not meant to restrict your genuine and work related use of what is an important method of communication and engagement. By its nature though, it is fast and responsive so when a mistake is made it can rapidly get out of control.

If you think social media may help your service you should contact the Head of Policy and Communications who can support you and ensure your proposal is supported by the other work being done as part of the corporate communications strategy.