



Derby City Council

# Electronic Communication and Social Media Policy

## Contents

1	Background and Scope.....	2
2	Understanding the Risks of Electronic Communications and Social Media .....	3
3	Acceptable Use and Monitoring .....	4
4	Official Communications.....	6
5	Social Media for Business Use .....	7
6	Personal Use of Social Media.....	9
7	Use of Electronic Communications and Social Media at work .....	10

# 1 Background and Scope

- 1.1. This policy is intended to provide clear guidance regarding the acceptable use of electronic communications and social media both within, and outside, of the work place.
- 1.2. The policy covers
  - All employees of the Council
  - All agency, temporary or contract staff working for the Council
  - All staff of third party suppliers contracted to and/or delivering services to the Council
  - All volunteers working with the Council on Council projects
  - All work placements
- 1.3. The policy does not cover elected members of the Council.
- 1.4. The Council recognises that electronic communications and social media are a reality and, when used effectively, can be used to support council business. We also recognise that their use can play an important role in the work-life balance of employees, agency workers, staff of suppliers and volunteers.
- 1.5. The Council had previously adopted a risk averse approach to such, for example, had blocked the use of social media within the work-place. There is increasing use of such for work related purposes, be this posting audio and video material on media streaming sites, professional and peer networking contact or communication with target audiences via their preferred social media channel.

## **2 Understanding the Risks of Electronic Communications and Social Media**

- 2.1. It is important that all staff understand the different risks involved with electronic communications and social media.
- 2.2. The use of electronic mail can be seen as a good way to communicate with individuals and with small groups as a user can control choosing who they include in the To, CC and BCC fields. However once a mail has been sent, even if it includes a privacy note and disclaimer, it can be easy for others to forward on to unintended recipients.
- 2.3. Exceptional care should be taken when using any social media tools, for example, websites and tablet/smartphone apps. Most social media sites work on the principle of broadcast by default, which means you cannot always control who may, or may not, see the content. Even where such sites allow users to set up privacy settings and to block unwanted contacts the content published may be broadcast beyond a controlled audience. The terms and conditions of such sites give powers and, in many cases, ownership of the published content to the social media site itself and not to the originator.
- 2.4. Clearer legal precedents have now emerged whereby the misuse of social media can result in both civil and criminal action and users of such need to have due regard for such consequences. Recent high profile cases have shown the dangers and led to both significant fines and imprisonment.
- 2.5. The Data Protection Act applies to the use of electronic communications and social media. Therefore, whether using such for work or personal purposes, you are advised to follow the principles of this Act when referring to any other living individual. Failure to do so could lead to enforcement action and potential civil or criminal action against the Council and/or against the individual responsible.

### 3 Acceptable Use and Monitoring

- 3.1. This policy sits with the Councils overall policies and as such, the Employee Code of Conduct applies and, the duty and obligations it imposes apply. Any action undertaken using electronic communications, including social media, which could be deemed a breach of the Code of Conduct, will be subject to investigation in the same way that similar action would be in other circumstances, for example, verbally in the work-place, on the phone or in public.
- 3.2. No data about individuals or organisations collected for Council use in the conducting of its business should be published or distributed via social media because:
  - we cannot control or secure the potential audience
  - we cannot ensure ownership of this data remains with the Council
  - we have to comply with UK and European laws that state all such data has to be held on servers in approved locations – we cannot do so for social media servers
  - we have to comply with various compliance regimes, some by statute, and others in order to share data with partners
  - we have a duty of care to the data subject
- 3.3. Staff can share such data using electronic mail but only with recipients who have a valid reason to receive such information. In some cases there is a requirement, owing to the nature of the data, to use secure and encrypted email, and accordingly to follow the compliance rules for such. This data should never be sent or published outside of these controlled audiences and/or secure mail systems. These audiences may be other government agencies, partners involved in providing health and social care and such like, where in addition to the Data Protection Act local policies and regulations apply.
- 3.4. The Council will not undertake random monitoring of the use of electronic communications and social media. It will however respond where there are allegations of behaviour that could breach the Code of Conduct, and will inspect logs and audit trails of internet activity if appropriate.
- 3.5. The Council reserves the right to monitor and maintain audit trails of some forms of electronic communications including email sent using Council email addresses and posting on social media pages set up for official council use.
- 3.6. The Council cannot monitor use of electronic communications or social media set up by individuals and not in the name of the Council. However where items are published electronically that make reference to the Council, to

Council business, or to named employees of the Council in their Council role, the Council may respond to such where it is brought to our attention.

## 4 Official Communications

- 4.1. The Council's policies and procedures for official communications and for Officers or Members authorised to issue press statements, apply equally to electronic communications and social media. Only those with delegated authority to issue such statements should use electronic communications and social media to do so. If using social media for such a communication, consideration must be made to the nature of the media and whether that communication is intended for broadcast publication.
- 4.2. Before any official public statement or communication intended as a press release or in response to an enquiry from the media is issued, it **must** be checked with relevant Officers in the communications team and authorised by the appropriate Manager and/or Elected Member.
- 4.3. Official communications that are prepared in advance, with an embargo set, must not be published using electronic communications or social media before the embargo date and time.
- 4.4. It is important that we continue to have effective internal Council communications that allow us to share important information with staff and others on a basis of trust and confidentiality. Such communications include :
  - the In Touch staff and managers bulletins
  - the team brief cascade
  - departmental or service newsletters
  - content on the i-Derby intranet and content on extranet sites set up with partner organisations.

No content published or distributed as an internal communication or as a communication with or between trusted partner(s), can be copied or republished via electronic communications or social media without explicit authorisation by an officer with the appropriate delegated powers.

## 5 Social Media for Business Use

- 5.1. The Council will allow the use of social media for business purposes as defined in this policy. Indeed, where the use of social media benefits the Council and/or our engagement with customers, it is encouraged. Examples of such include:
- To participate in peer and professional body networks
  - To engage with partners who use social media
  - To access and communicate with customers who may have a preference for social media as a communications tool - see below
  - To access content that is for business use that has been posted or published via social media
- 5.2. The Council has a duty to protect itself and its reputation with the community and wants to use social media in a way that is consistent with the overall Communications policy and protocol.
- 5.3. If you want to set up a new social media forum for engaging with customers you need approval to do this and you need to agree to some policies and rules for the management of such social media sites. The communications team need to be consulted and to give approval to each such channel and will provide advice on what is required and how the site should be branded. The use of such sites will be monitored.
- 5.4. You should not use a separate social media site to publish content that could and should be published on the corporate website. If you wish to use social media to extend the reach of such content then it should be published on the website including links to it within social media sites and postings.
- 5.5. If you are signing up to use any social media facility for business use you should use your Council email address and give your job title. You must not use any alias or any avatar that could make your communications anonymous. Our customers and others have a right to transparency and openness. Do not forget that you represent the Council when doing so.
- 5.6. Any items you publish or post and any material you access must be relevant to your role at the Council and could be considered to be made on behalf of the Council. In the same way that you are responsible for your actions by email, on the telephone or when wearing your Council ID badge, you are responsible for your actions, views, opinions and any published comments on social media. Therefore the same standards of behaviour are essential.
- 5.7. On some social media sites making a note that your comments and postings represent your personal opinions and not those of the Council may be possible. If this is possible you should do so in the same way as our external

emails which have a disclaimer added when they are sent. However, even if you do this, what you post will reflect on the Council and doing such does not reduce your responsibility to follow the employee Code of Conduct.

## **6 Personal Use of Social Media**

- 6.1. The Council cannot and does not want to prevent or restrict your use of social media in your own time and for your own purposes.
- 6.2. However the Council needs to make all users aware that if their personal use of social media conflicts with the duties for the Council, or their obligations as an employee, as contracted suppliers, or a volunteer, then the Council has the right to take appropriate action.
- 6.3. No information that you have as a representative of the Council should be copied, published or commented upon when using social media for personal use.
- 6.4. The Council's standards and codes of behaviour extend beyond the workplace in respect of any actions or communications you may engage in that could bring the council into disrepute.

## **7 Use of Electronic Communications and Social Media at work**

- 7.1. The Council will not block access to social media and media streaming sites at work; but will block sites whose purpose and content are not consistent with the Council's values and policies.
- 7.2. Personal use of social media sites is only permitted in your own time, any time spent on personal use of social media should be recorded as non working time.
- 7.3. If you are suspected of using social media for personal use during working time then, just as carrying out other personal activities in work time, you may be subject to investigation and potential disciplinary action.
- 7.4. If there is widespread abuse of social media during work time, or it is accessed from Council computers, or via the Council internet gateway, then we may have to re-impose blocking controls on such sites.
- 7.5. You must never seek to download or run any application or to install any software onto or from a council computer via social media. Such sites are often used by others to propagate viruses or other malware.
- 7.6. If you access a site or content on social media that you realise is inconsistent with Council policies then you should report this to your line manager immediately. Where possible we will seek to block such sites from future use.
- 7.7. If you access a site, or content on social media, or you receive emails or other electronic communications that you believe are in breach of the Council's values, policies and/or code of conduct or that may be attacking or damaging to the Council's reputation, then you have a duty to report them. You should not reply to any such content or emails directly.
- 7.8. Your use of social media and other electronic communications whether for work or personal use must be consistent with the standards of behaviour expected by the Council at all times, and must be legal. Such use can be traced to the Council's internet gateway and as such the Council has obligations which can include assisting in any criminal investigation or responding to the Information Commissioners Office or other regulatory bodies.