MERSEYSIDE WASTE DISPOSAL AUTHORITY

Social Media Policy

1.0 Introduction

1.1 Purpose (aim of policy)

1.2 Scope

2.0 Policy Statement

3.0 Policy Details

3.1 Responsibilities of Officers

3.2 Use by Members

3.3 Investigatory Use

3.4 Personal Use

4.0 Relationship with other corporate strategies and policies

5.0 Breaches in Policy

5.1 Equality and Diversity

5.2 Criminal Activities

5.3 Obscene Publications

5.4 Code of Conduct

6.0 Information and Training

7.0 Monitoring

1.0 Introduction

As information and communications technology continues to move forward, making considerable advances, so too do the tools that enable us to communicate with, and unite people. 'Social Media' is the term used for the current wave of online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests. Social media involves building online communities or networks, which encourage participation, dialogue and involvement.

Social media is at the forefront of modern communications; its capabilities are already being exploited by central government and local government and various public and private sector organisations as a method of engagement with customers, stakeholders and partners.

We can benefit from taking a similar, innovative approach to communicating with people, which can lead to greater involvement with service users, increased efficiencies and improvement in our reputation.

For social media to work effectively it is vital that it is used as part of the overall communications mix: up to date information about the Authority, its services and engagement activities.

There are many social media sites and we need to set clear guidelines for the use of those social media sites to ensure they are used effectively as part of a wider communications mix and that their use does not expose the Authority to security risks or reputational damage. Therefore, we need a comprehensive policy to effectively manage and regulate the corporate use of social media.

1.1 Purpose and Aim of Policy

Social media offers great potential for building relationships and improving the services that we provide. The potential of social media as a business tool is almost limitless, however if misused, it has the potential to cause considerable damage to the Authority and those we seek to engage with. This policy will clearly set out how social media can be managed effectively and how any risks or pitfalls can be avoided or mitigated.

As with any other online activity, there are often risks associated, the following types of risk that have been identified with social media use are:

- Virus or other malware (malicious software)
- Disclosure of confidential information
- Damage to reputation
- Social engineering attacks (this is the act of manipulating people into disclosing confidential material or carrying out certain actions)
- Civil or Criminal action relating to breaches of legislation
- Breach of Safeguarding.

The purpose of this policy is to ensure that where the Authority uses social media, it does so in a controlled manner that enables us to engage safely and effectively with our employees, partners and the people that use our services.

The aim of this policy is to ensure:

- Engagement with individuals and partner organisations and successful promotion of Authority services through the use of social media
- A consistent and corporate approach is adopted and maintained in the use of social media
- That Authority information remains secure and is not compromised through the use of social media
- That authorised users operate within existing policies, guidelines and relevant legislation
- That the Authority's reputation is not damaged or adversely affected.
- That the Authority is not exposed to legal and governance risks that can be significant.

1.2 Scope

Only employees authorised by the Chief Executive are permitted to post material on a social media websites in the Authority name and on its behalf.

All employees have the ability to access social media sites however, a business case is required for those sections and staff wishing to have access to the Authority's corporate website accounts and online tools.

This policy applies to all employees of the Authority and elected Members.

Use of social media applications by employees or Members for personal use is addressed in this policy (see 3.2). Officers and Members should also refer to the respective Code of Conduct and the Internet and E-Mail Policy which makes clear that when using the internet (which includes social media) for personal reasons you should not publish defamatory and/or knowingly false material about the Authority, your colleagues and/or our partners. You should not publish anything which may have the potential through association to bring the Authority into disrepute. Any harassment, intimidation or bullying of colleagues, managers or other employees while using social media will not be acceptable.

Contractors, third parties and partners are also expected to ensure that private use of social media by their employees will not be conducted in a way which could damage the reputation of the Authority or could be considered harassment, intimidation or bullying of Authority employees or Members.

2. Policy Statement

It is acknowledged that there is significant potential for using social media and that this can bring great advantages. The responsible, corporate use of social media is therefore encouraged.

This policy provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise the Authority information or computer systems/networks.

Users must ensure that they use social media sensibly and responsibly, in line with corporate policy. They must ensure that their use will not adversely affect the Authority or its business, nor be damaging to the Authority's reputation and credibility or otherwise violate any Authority policies.

3. Policy Details

Social media will be made available for corporate, business use only, subject to approval for using such communications.

3.1 Responsibilities of Officers

The following guidelines will apply to online participation and set out the standards of behaviour expected as a representative of the Authority. Officers of this Authority should always ensure that political impartiality is observed when undertaking any form of online participation.

1. Be aware of and recognise your responsibilities identified in the Social Media Policy.

2. Remember that you are personally responsible for the content you publish on any form of social media.

3. Never give out personal details such as home address and telephone numbers. Ensure that you handle any personal or sensitive information in line with the Authority's Data Protection Policy.

4. Be aware of Safeguarding issues (e.g. particularly in relation to sharing photos without parental consent), as Social Media sites are often misused by offenders. Safeguarding is everyone's business – if you have any concerns about other site users, you have a responsibility to report these to a Manager.

5. Respect copyright, fair-use and financial disclosure laws.

6. Social media sites are in the public domain and it is important to ensure that you are confident about the nature of the information you publish. Permission must be obtained if you wish to publish or report on meetings or discussions that are meant to be private or internal to the Authority. Don't cite or reference service users, partners or suppliers without their approval.

7. Don't use insulting, offensive, racist, sexist or homophobic language or engage in any conduct that would not be accepted in the workplace. Show consideration for others' privacy and for topics considered objectionable or inflammatory – such as politics or religion.

8. Don't download any software, shareware or freeware from any social media site, unless this has been approved.

Failure to comply with the guidelines could result in disciplinary action being taken.

3.2 Use by Members

Members should ensure that they are familiar with the guidance that is set out within this policy and that their use of social media does not put the Authority's information and security systems at risk, or be damaging to the reputation of the Authority. Members should also be familiar with the Members' Code of Conduct, which outlines key information and guidance.

Members should be aware that any reports of inappropriate activity on social media (either through corporate or personal use) linking them to the Authority, will be investigated.

3.3 Investigatory Use

It is recognised that social media can be used for investigatory purposes, such as identifying fraud, illegal events etc. It is important that employees who use social media for this purpose comply with relevant guidance and legislation.

3.4 Personal Use

This policy relates to the business use of social media but also covers some areas of personal use of social media. If employees (that have been granted access to corporate social media) are found to be accessing social media sites for personal reasons, then appropriate action will be taken. Employees who access social media sites during their own time (e.g. during lunch break or outside of work time) must also be aware that inappropriate activity linking them to the Authority will be investigated and action may be taken.

Employees should be aware that the Code of Conduct for Officers covers the use of fidelity and information disclosure, and should bear this in mind when using social media (in a personal capacity) outside work. Employees should be aware that any reports of inappropriate activity linking them to the Authority, will be investigated and action may be taken.

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.

4. Relationship with other corporate strategies and policies

This policy also links to (and should be read in conjunction with) the following policies:

- The Internet and Email Policy
- The Code of Conduct for Officers
- The Publication Scheme(with reference to Data Protection)The Communications Strategy
- The Code of Conduct for Members
- The Disciplinary Procedure

5. Breaches in Policy

5.1 Equality and Diversity.

Social Media must not be used in an abusive or hateful manner, or in such a way that breaches the Authority's obligations under equality and diversity legislation. (Race Relations (Amendment) Act 2000)

This includes the content of both public and private social media tools. It includes messages, images or other information that may be posted by Authority representatives. Importantly, it also covers the hosting of posts by other parties on social media sites relating to Authority activity.

Where the Authority receives electronic material through social media that is in contravention with legislation in respect of Hate Crime, or incitement to such, we will report this to the Police without hesitation or exception.

5.2 Criminal Activities

The Authority is bound by the legislative requirements of the Anti-Terrorism Crime and Security Act 2001 to report to the police any activity, or suspicion of activity relating to terrorism or incitement to such that may arise through our use of social networking tools.

The Authority may also share with Police any information regarding actual or potential criminal activity of any kind received through social media.

5.3 Obscene Publications

The publication of obscene material is prohibited by the Obscene Publications Act 1959: the Protection of Children Act 1978 and the Criminal Justice Act 1988.

5.4 Code of Conduct

Social media must not be used in a manner that breaches the Authority's misconduct and bullying and harassment policies

Employee use of social networking tools either during the working day for business purposes or during their rest break or lunch periods is governed by the internet and email policy and the Employee Code of Conduct.

6. Information and Training

All employees of the Authority will receive appropriate training on the implementation and use of this Social Media Policy as part of the Corporate Training Plan

The policy and any associated documentation will be available for all employees to access in the controlled document library.

7. Monitoring

The Authority will ensure that no material is published, either by ourselves or by third parties that will contravene our responsibilities under this policy.

Use of social media for Authority business will be limited to those users authorised to post material on behalf of the Authority and will be accountable for the quality and content of this material under the terms of this Policy when determining where and when they post that material.