SOCIAL MEDIA PROCEDURE

1. Our Policy

1.1 Social media is at the forefront of modern communications. It is acknowledged that there is significant potential for using social media. It can bring advantages, including greater involvement with Council customers, stakeholders and partners; increased efficiencies; and improvement of the Council's reputation. The responsible, corporate and personal use of social media is actively encouraged.

1.2 The use of social media can be managed effectively and the risks or pitfalls can be avoided or mitigated.

1.3 This procedure provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise Council information or computer systems or networks.

1.4 Users of social media must ensure:

- that they use social media sensibly and responsibly, in line with corporate policy;

- that the use of social media (See Appendix 1 for definitions)

  - will not adversely affect the Council or its business;
  - will not damage the Council's reputation or credibility;
  - will not breach any Council policies.

2. The Purpose of this Procedure

2.1 This procedure is intended to provide:

- guidance for employees on the safe and appropriate use of social media;
- details on how the Council will monitor usage;
- details of the process and consequences where there has been a breach in the use of the social media.policy

2.2 This procedure should be read and interpreted in conjunction with other Policies:

  - Acceptable use policy for Internet service users
  - Supporting documentation: FAQs and jargon busting
  - Equality in Employment Procedure
  - Unfair Discrimination Bullying and Harassment Procedure
  - Employee Code of Conduct

2.3 The procedure applies to all employees and other users, including agency workers, contractors and partners, who use the

Council's IT infrastructure or who manage social media services or accounts on behalf of the Council.

3. Principles of this Procedure

3.1 Responsibilities of Employees

The following will apply to online internet participation. It sets out the standards of behaviour expected as a representative/employee of Luton Borough Council. Individuals should:

a) Be aware of and recognise their responsibilities identified in this Procedure.
b) Remember that they are personally responsible for the content they publish on any form of social media.
c) Never give out personal details such as home address and telephone numbers of colleagues. Ensure that they handle any personal data or sensitive information in line with Council policies (see Appendix 2).
d) Respect copyright, fair-use and financial disclosure laws.
e) Ensure that they are confident about the nature of the information they publish. Permission must be sought from their line manager if they wish to publish or report on meetings or discussions that are meant to be private or internal to the Council.
f) Not cite or reference customers, partners or suppliers without their approval.
g) Not use insulting, offensive or racist language or engage in any conduct that would not be acceptable in the workplace.
h) Show consideration for others' privacy and for topics that may be considered objectionable or inflammatory- such as politics or religion.
i) Not attempt to download or install any software applications or executable software from any social media site, unless this has been approved and authorised by Civica.

This list is not exhaustive.

3.1.1 Safeguarding

What is Safeguarding?

Safeguarding is a requirement for Luton Borough Council to ensure that children and vulnerable adults in receipt of Council services are safe from harm.

Employees should be aware of Safeguarding issues, as Social Media sites are often misused by offenders. Safeguarding is everyone's business, if employees have any concerns about other site users, they have a responsibility to report these to:

1) Safeguarding Children email: ~LBC Initial Assessment Team
2) Safeguarding Adults email: ~LBC Access and Assessment

3.1.2 **Interaction with Problem Users or Groups**

In a small number of cases access to social networking sites may be required to monitor the activities of events, groups or persons that pose a risk to others or are involved in criminal or fraudulent activity. Employees must avoid direct interaction with such people. By interacting e.g. becoming their friend on Facebook employees may be placing themselves or others in a position of personal risk. (See Appendix 2 for further guidance on using social media safely).

3.2 **Responsibilities when using Social Media in an Official Capacity**

3.2.1 Employees and others who use social media must be aware of and comply with the Acceptable use policy for Internet service users.

3.2.2 Service areas looking to make use of social media in an official capacity should in the first instance contact the Web Team by email: ~LBC Web Team. There is no 'one-size-fits-all' approach, as different departments have different aims and objectives. The most appropriate strategy needs to be agreed to allow the service to make the best use of their resources, and the skills and experience of those already using social media within the Web Team and across the Council.

Council departments are encouraged to make use of social media providing they have seriously considered:

- Why they want to do it and what benefits they will get;
- What information they have to share;
- Who in the department is going to manage their presence;
- How they will fit daily monitoring and updates into their work schedule

All these considerations should be discussed with the Web Team who can provide guidance and support in using these tools and also ensure any social media dialogue, interaction or content is integrated within the services established web presence.

This collaborative approach will help build and share the Council's collective knowledge as we learn how to harness these tools effectively to transform service delivery as well as keeping pace with the emerging technology.

3.2.3 Employees and other users must identify themselves as being part of Luton Borough Council. The Web Team will advise on the best way to do this depending on the tool being used.

3.2.4 If an employee or other user receives any threats, abuse or harassment from members of the public through their use of social media then they must report such incidents to their Head of Service.

3.2.5 Audit and Inspection of ICT Equipment

The Council may at any time and without notice, request software and hardware audit or inspection (used at work or remotely). Employees may therefore be required to surrender ICT equipment at short notice and must co-operate fully with any such audit or inspection.

3.2.6 Access to Personal Information during an Inspection

Where the inspection of ICT equipment is authorised in relation to an alleged breach of policy or standards, employees' personal e-mails and other non-work related data e.g. family photos, personal letters etc, resident on the equipment may be retrieved and reviewed. If this information is deemed relevant to the investigation, it may be used as evidence.

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 those employees who use social media for these purposes comply with the relevant guidance and legislation.

3.4 Responsibilities when using Social Media for Personal Use

3.4.1 Employees should be aware that any reports of inappropriate activity linking them to the Council will be investigated.

3.4.2 If employees use social media outside of Council working hours and in their private life, they **should not** set up clients and customers, for example, vulnerable people or children, as friends or associates. See Para 3.1.1 regarding Safeguarding. With the rise in identity related fraud, employees may wish to limit the amount of personal information that they display on their personal profile.

3.4.3 Employees should not use the Council logo on personal web pages.

3.4.4 Sensitive information must not be posted on social networking sites. See the Information Classification and Handling policy.

3.4.5 Employees should not include contact details or photographs of service users or staff without their permission.

3.4.6 Under no circumstances should offensive comments be made about the Council, Members, customers or work colleagues. This may amount to cyber-bullying or defamation and could be deemed a disciplinary offence.

Failure to comply with the above guidelines could result in disciplinary action being taken in line with the Council's Disciplinary Procedure.

4. Management Responsibilities

Responsible Officers, e.g. Heads of Service, line managers and the Council's Web and Communications Team, have a duty to ensure that users comply with the Social Media Procedure and relevant guidance and do not abuse their rights or misuse such sites. Any breaches of this procedure by employees should be dealt with immediately and in accordance with Council procedures.

5. Monitoring Arrangements

5.1 The use of social media will be **monitored to ensure compliance** with Council policies and guidelines, and to support security and criminal investigations,

5.2 The Council reserves the right to shut down any corporate social media accounts that have become dormant or breach this procedure.

5.3 Reporting Arrangements

Any potential misuse of social media identified by Human Resources, Web team, the Information Governance Officer, Communications Team or others, will be reported to the appropriate officer or body.

5.4 Performance Measures

Records of user activity, provided by Civica**,** will be reviewed to ensure compliance with Council policies and standards.

6. Breaches of Policy

Any breaches may lead to access being withdrawn and disciplinary action being taken. Serious breaches of this procedure will amount to gross misconduct and may result in dismissal.

Other violations of this procedure, such as breaching the Data Protection Act 1988 could lead to fines being issued and possible criminal or civil action being taken against the Council, the individual(s) involved, or other organisations (e.g. 3rd party contractors).

7. Legal Requirements

The following legal documents have a bearing, or impinge on the rationale of this procedure:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998

What is Social Media?

Social networking

Websites where you create a personal profile then chat, discuss and share information with others such as friends and family. Organisations can also create profiles and promote campaigns and events. Example www.facebook.com

Why are social media sites free?

Many such sites resell your personal information e.g. birthdays, address, phone number, likes, dislikes, memberships, home town etc to other companies. These companies in turn send you targeted advertisements and offers. So before you put personal data on a social media site; ask yourself how much of it you are happy to share with others.

Wikis

These sites enable users to create, edit and share information about a subject or topic. Example: www.wikipedia.org

Blogs

These are internet diaries, sometimes encompassing forums that allow you to give advice, ask questions or comment on what others have said. The content of a blog may vary from the mundane through to highly specialised. These sites are available to Council and Trust users with internet access.

Twitter

A mechanism for broadcasting short messages; these can include hyperlinks or photos. The broadcasts, known as 'tweets', go only to your 'followers'. Followers are persons who have expressed an interest in what you are saying. It's an ideal medium for keeping you, your team or your party up to date with the latest news on key topics, especially when Twitter is loaded as a mobile phone application.

Video sharing

Where you upload and share your personal videos with the rest of the web community. Example www.youtube.co.uk

Photo sharing

You can upload pictures and images to a personal account which can be viewed by web users the world over. Example www.flickr.com

News aggregation

News aggregators provide a list of the latest news stories published by users from a range of different websites. Example: www.digg.com

Consumer choice

Many sites give you an opportunity to post your views on a product or service and to check what others think before you buy. Example: www.tripadvisor.org

Appendix 2

Top Tips for using Social Media safely

Facebook, Twitter, LinkedIn and all the rest are great. Take a look at these top tips to avoid opening the door on data loss, identity theft and malware infection.

Know the rules

Make sure you know where to find the Council's policies and guidance. –See Home page of intranet-bottom

Use secure passwords

What's behind a password? …Your life!
If it's cracked, your life's for sale. Make it really secure – ideally you should use at least 14 characters and mix in upper and lower case, numbers and symbols.

Check default settings

Social media sites have large numbers of connected users. Make sure you check each site's default settings so your details aren't on public display and minimise the amount of personal information you provide.

Be picture prudent

Be careful what pictures you show and try to avoid adding compromising or embarrassing images that might harm you, your organisation or your customers.

Beware of Big Brother

Using social media sites as a diary is OK if you want family, friends (and enemies) and anyone else to know everything about you.

Secure your computers

Your life is valuable, as are our customers and employees! Hackers want our data. So only use computers with up-to-date security software and effective firewalls.

Think before you click

Never click on links just because you know the sender – some malware takes control of other user's accounts and then automatically sends infected messages to you and other contacts in an attempt to infect them. If the email looks dodgy it probably is.

Stranger danger

Be wary of anyone trying to get your details by sending unsolicited invitations, friend requests or applications. If you don't know the person, the best thing to do is to ignore the request.