West Lothian Council

Internet, Social Media and Email Policy

Approved : **Council Executive 25 June 2012**

DATA LABEL: PUBLIC

INTERNET, SOCIAL MEDIA AND E-MAIL POLICY

(Covering all Employees)

CONTENTS

1. POLICY STATEMENT

Council employees are expected to use Internet, Social Media and E-mail systems effectively and responsibly and in accordance with approved operational and security standards while in the course of their work. Employees equally have a responsibility to ensure that their private use of internet, social Media and e-mail out with the workplace does not impact adversely on the council and its business, compromise their contractual relationship with the council or breach council policy.

This policy sets out the expected standards of internet, social media and email use and provides for those standards to be monitored and enforced. The content should be read in conjunction with the relevant employment policies referred to in this document together with other policies and guidance issued by the council's IT Service, in particular the Data Protection and Information Security Policies.

2. POLICY AIMS

The key aims of the policy are to:

- regulate and control access to the council's internet, social media and e-mail system networks;
- promote efficient and effective use of Internet, social media and e-mail facilities while allowing reasonable and limited personal use in an employee's own time;
- set standards for the proper secure and lawful use of internet, social media and e-mail in order to minimise and manage the potential risks to the council from inappropriate and illegal use;
- provide employees with guidance on their responsibilities when accessing the internet via the council networks and when using social media and council email applications.

3. SCOPE

This policy applies to the use of internet, social media and e-mail in the following circumstances:

Business Use:-	Use for legitimate council business consistent with the duties and responsibilities of an employee's post.
Personal Use:-	Limited personal use at an employee's place of work out with working hours.
Private Use:-	Private use out with work in an employee's own time which may have an impact on the council or on an individual's employment with the council.

4. SOCIAL MEDIA

'Social Media' is the collective term commonly given to websites and web applications that are used to discuss, debate and share information on - line. The most common types are: social networking, blogs, micro-blogging, content communities, wikis and forums, examples of which include, Facebook, Twitter, Linkedin, YouTube, Flickr and Wikipedia.

The need to ensure that Social Media sites are used responsibly, legally and with due regard to the provisions of other relevant council policies and codes of conduct applies equally to business, personal and private use.

5. LEGAL LIABILITY

The council may be held liable for any statements made, or contractual arrangements entered into as a result of an employee's use of internet, social media or e-mail for business use. Vicarious liability may also extend to illegal or unlawful activities carried out by employees during personal and private use which can be linked to the council.

To prevent the council and employees individually becoming exposed to legal liability (and possibly criminal proceedings), employees must not engage in conduct likely to contravene any of the following:

Data Protection Act

- The unauthorised or unlawful processing of personal data and accidental loss or destruction of, or damage to, personal data by an employee could result in a breach of the Data Protection Act 1998. It is a criminal offence for the council or an employee to allow access to, or alteration of, or to disclose personal data without authorisation. The Council's Information Security policy sets out the appropriate technical and organisational measures that are in place to safeguard against such breaches.

  Further information on the Data Protection Act can be obtained on the Council's intranet or from the Information Liaison Officer (ILO) assigned to the service concerned.

Freedom of Information & Records Management

- The public have the right to request any kind of recorded information from the council subject to some exemptions. This includes all information recorded on emails which is therefore open to public scrutiny. Therefore employees must ensure appropriate use of email and create and keep accurate records in line with the council's Records Management Policy. Further information relating to Freedom of Information (FOI) and the council's Records Management Policy can be obtained on the Council's intranet or from an Information Liaison Officer (ILO).

Intellectual Property/Copyright Infringement

- The unauthorised copying, distribution or possession of intellectual property (copyright material, designs, patents, trademarks, inventions, ideas, know - how, business information and lists). These activities are an infringement of copyright and are strictly forbidden. Copyright works include text, graphics, still images, computer software, music and video clips. Any unauthorised copying of those materials by an employee could render the employer liable under civil and criminal law.

Obscenity and Pornography

- Accessing, downloading, displaying on screen or transmitting material with a sexual content could constitute criminal offences for which both the council and employee may be liable.

Defamation

- Communicating a defamatory (untrue) statement about another individual either within or out with the council. The council and the employee personally could be sued for damages and criminal penalties could also apply.

Harassment and Discrimination

- Communication of offensive remarks, for example, the distribution of sexually explicit or offensive material relating to an individual's personal characteristics, perceived characteristics or those of someone connected to them as defined within equality legislation. These actions are capable of forming the basis of a complaint of harassment and bullying and liability can fall on both the council and the offending employee.

6. ACCESS TO COUNCIL INTERNET, SOCIAL MEDIA & EMAIL FACILITIES

To ensure information security, it is necessary to regulate not only those employees who will have access to the council's Internet, social media and email systems but also the purposes for which such access is granted.

In order to gain access to the council's Internet, social media and email systems, employees must complete the access registration process. Access to systems will be authorised on the basis of business need as determined by Service Managers.

Following completion of the Internet & Email Access Request Form, a copy of the form must be retained by the line manager.

By completing the User Declaration on the Internet & Email Access Request Form, employees automatically give the council consent to carry out reasonable monitoring to ensure compliance with the policy, security of the system and for the prevention and detection of crime.

7. AUTHORISED USE OF COUNCIL INTERNET, SOCIAL MEDIA & EMAIL FACILITIES

Business Use

Authorisation for employees to use Internet, social media and email systems for council business will depend on service need and the nature of the duties and responsibilities of their posts.

<u>E- Mail</u>

Emails are official council records. Staff must manage email with, and in the same way as other council records i.e. filed and stored on the EDRM system. Email must be handled as per the Information Handling Procedure and therefore must be

classified with an appropriate data label. Staff must observe the security implications required by the sensitivity or confidentiality of information or data contained within each email. Email messages are subject to Data Protection, Freedom of Information and Public Records legislation.

For security and confidentiality reasons, employees must never use personal e-mail accounts for the purposes of transmitting information relating to council business or forward email relating to council business from council mailboxes to personal email accounts. Where there is a requirement to communicate information relating to council business to or from external locations, for example, during periods of occasional home–working as part of contingency arrangements during severe weather, only secure systems such as Webmail and Blackberry, approved in accordance with the council's Information Security Policy must be used. Non secured devices such as personal smartphones, i-phones and androids must never be connected to the council network or mail system. Further guidance on security of information and confidentiality is set out in Section 12 of this policy.

Social Media

Only official use of council social media sites is authorised during work time. These sites are set up within council guidelines and operated by staff who are trained in their use. A business case must be in place for access to other official social media sites eg partner organisations, professional bodies, suppliers etc.

Employees who are authorised to use social media facilities for business purposes must ensure that usage does not infringe the terms of the council's Code of Conduct for Employees, Disciplinary Code and Bullying & Harassment Policy & Code of Practice.

Heads of Service are responsible for approving the setting up of online accounts for the purposes of accessing social media facilities.

An officer should be nominated who has responsibility for monitoring the site and approving the content. All account names and passwords along with the name of the responsible officer should be provided to IT Services to be included on the Asset Register. Email: itservicedesk@westlothian.gov.uk

Personal Use (using council facilities)

It is emphasised that although Internet, social media and e-mail facilities are provided primarily for business use, employees may use the systems for occasional personal use.

Personal use of Internet, social media and e-mail systems is subject to the following conditions:

- personal use must be reasonable and should take place in an employee's own time but in any event must not take priority over their work responsibilities;
- personal use is subject to the same rules that apply to business use and as such must not fall within the categories of use prohibited under this policy;
- the performance and effectiveness of the council's Internet, social media and email systems as a business tool must not be reduced, disrupted or in any way compromised by the level or nature of personal use;

- personal use must not incur the council in any unauthorised expenses;
- all personal e-mails must be deleted from the system as soon as possible;
- employees must consider the council's reputation when sending personal emails or when taking part in on-line discussions/forums and must ensure that it is made clear that they are not commenting in an official capacity and that the views expressed are their own and do not necessarily reflect the views of the council.
- the council does not accept responsibility for security of personal or personal financial information or transactions sent or retrieved via the Internet or on council networks.
- Council email accounts must never be used to register with any non-official social media sites.

8. PRIVATE USE OF INTERNET, SOCIAL MEDIA & EMAIL

The council respects an employee's right to freedom of expression when privately using the Internet, social media and email out with the workplace in their own time. Employees should however, be careful to ensure that they do not inadvertently or otherwise engage in online conduct that could undermine their contractual obligations as an employee of the council.

Employees are reminded that they must observe the Council's Bullying & Harassment Policy, Disciplinary Code, Code of Conduct, Information Handling Procedure, Records Management Policy, and Information Security Policy while using the Internet, social media and email both within and out with the workplace.

Information posted on social media sites is in the public domain regardless of privacy settings. The author is responsible for the information posted and is legally liable for any breach or omission arising from his/her actions.

The council's policy in so far as it relates to private use of Internet, Social Media and Email, is underpinned by the following considerations:

- In common with the conditions governing the use of internet, social media and e-mail for business and personal purposes, employees must observe the council's Code of Conduct for Employees, Disciplinary Code, Bullying & Harassment Policy and Information Security Policy.
- Employees are encouraged not to comment on their work or make reference to the Council on external web pages. If they choose to do so, they must make it clear that they are not commenting in an official capacity, and that the views expressed are their own and do not necessarily reflect the views of the council.
- Should employees become aware of negative or disparaging remarks about the Council or its services, they should not respond but instead advise their line manager who will determine if the comments merit a referral to the Corporate Communications team.
- Employees should be aware that colleagues, customers and third parties often have access to the material they may post on the Internet and as such this should be kept in mind when publishing information online that can be viewed by more than friends and family.

- Employees must never communicate or disclose information online in breach of the council's Data Protection or Information Security Policies or take up public positions on issues that are counter to the council's interests.

- Many social media sites have the facility for users to write reviews, recommendations or referrals for individuals, businesses or services. If writing a review, recommendation or referral, employees must ensure that it is clear that they do so as an individual, not as an employee or official representative of the council. By creating the false impression that the council endorses an individual, business or service could result in the council inadvertently incurring a legal liability.

9. BULLYING & HARRASSMENT AT WORK

The Policy and Procedure on Dealing with Complaints of Bulling and Harassment at Work along with the associated Code of Practice applies to all employees during working hours and outside normal working hours in the course of employment where an individual employee's action detrimentally affects the council or another council employee.

Use of the Internet, Social Media or E-mail in a manner that harasses, bullies, intimidates or threatens a council employee whether within or out with work is a contravention of the Bullying & Harassment Policy and Disciplinary Code and therefore may result in disciplinary action being taken under the council's Disciplinary Procedure.

10. PROFESSIONAL CONDUCT AND STANDARDS

It is essential that professional standards are strictly observed when using Internet, Social Media & E-mail for business purposes. This is particularly so for employees who handle sensitive and confidential information relating to clients which may be shared internally or externally and which may be the subject of access by professional inspection agencies on a routine basis.

Business e-mail communications must comply with service standards and should not use language of an over familiar, colloquial or unprofessional nature. Guidance in respect of the general standards expected of employees is contained within the council's corporate Communications Strategy document entitled the 'West Lothian Way' that can be accessed at West Lothian Way.

Employees registered with professional bodies such as Scottish Social Services Council (SSSC) and the General Teaching Council for Scotland (GTCS) must ensure that their use of the internet, social media and e-mail does not compromise or breach the standards of professional conduct expected of them.

Employees must ensure that they do not overstep professional boundaries by communicating with or 'befriending' clients/customers/pupils on social networking sites out with communications necessary for the purpose of carrying out their professional duties. The council recognises the Glow Scotland website as an approved site for communicating with pupils.

11. UNAUTHORISED USE

A comprehensive list of expressly prohibited activities is set out within the Appendix to this policy. Engaging in such activities may result in disciplinary action being taken against the individual concerned, up to and including dismissal in accordance with the council's Disciplinary Code.

12. MONITORING

General

The council will log and monitor its Internet, social media and e-mail systems for the following legitimate business purposes:

- to prevent or detect crime (e.g. fraud/corruption/hacking);
- to investigate or detect unauthorised use as stipulated within this policy;
- to ensure effective operation of its systems (e.g. combating and prevention of viruses);
- to investigate or contain an information security incident;
- to find or retrieve messages/records that have been lost or misfiled.

In consenting to the terms on which they are authorised to use the council's internet, social media and email systems (including limited personal use), employees are also acknowledging the fact that their right to privacy is restricted by the council's right to log and monitor usage for the above purposes.

E- Mail

- The council reserves the right to log the senders, recipients and contents of all e-mail messages transmitted through its systems;
- The council also reserves the right to inspect the content of any employee's incoming or outgoing e-mails, subject to such inspection being carried out only with good cause and for the detection of misuse, crime, fraudulent or defamatory statements;
- On a monthly basis, users logging on to the e-mail system will receive an automatic on-line reminder of the consequences of misuse of the system and of the fact that logs are kept of e-mail usage and that they do not have a completely unrestricted assumption of privacy when using the system;
- In line with the Data Protection Act users are entitled to inspect files or logs of their e-mail usage held by the council and can do so by submitting a Subject Access Request in writing.
- In the event of alleged misuse of the system, files or logs of e-mail usage may be forwarded to the employee's line manager. The information may also be made available to an officer appointed to investigate alleged misuse, in accordance with the council's Disciplinary, Grievance and Bullying & Harassment procedures where appropriate.

Internet & Social Media

- The use of the Internet and social media is logged and monitored as part of the council's information security function;
- If a user attempts to access one of the blacklisted websites, or one that contains banned words, an alert is sent to the System Administrator's e-mail account. Details of the inappropriate usage will then be examined by IT security staff;
- Where the alert mechanism indicates that a user has persistently attempted to gain access to inappropriate and banned sites, a log of the times and nature of the sites to which access has been attempted will be forwarded to the employee's line manager. This information may be used as part of an investigation under the council's Disciplinary Procedure.
- Monitoring of social media sites created for council business purposes is the responsibility of the relevant Service Manager in accordance with Section 13 of this policy.
- Employees should report to their line manager any instances of information being posted by another employee on websites or social media sites that could be considered offensive, libellous, or potentially harmful to employees, pupils, clients, service users or the council.

13. CONSEQUENCES OF MISUSE

Suspected misuse of the council's Internet, social media or e-mail systems will be investigated under the council's Disciplinary Procedure. Any resulting disciplinary action, and the level of that action, will depend on the extent of misuse identified in each case. Where substantiated, serious misuse including knowingly accessing or attempting to access, down-load, store or circulate offensive, pornographic or discriminatory material will be regarded as gross misconduct in accordance with the council's Disciplinary Code and will result in summary dismissal.

Disciplinary action will also extend to inappropriate, private use of internet, social media and e-mail out with the council that is considered to breach this policy and/or the council's Disciplinary Code, Code of Conduct for Employees, Bullying & Harassment Policy.

In certain circumstance, breaches of this policy could be deemed unlawful and the council will make appropriate referral to the Police.

When appropriate, referral will also be made to professional bodies such as the SSSC and the GTC for Scotland in accordance with the relevant procedures. In cases where the actions of employee's who are engaged in regulated work have resulted in harm or inappropriate behaviour toward a child or protected adult, the matter may be referred to Disclosure Scotland following appropriate investigation and disciplinary action.

14. CONFIDENTIALITY AND SECURITY

As an employer and provider of public services, the council holds personal, confidential and sensitive information about employees, citizens and clients. The council is, therefore, responsible for ensuring that its obligation of confidentiality to

those individuals is not compromised and that all such information is processed in accordance with Data Protection legislation.

All confidential or protected information should be kept secure and used only for the official purpose(s) intended. It must not be disclosed to any unauthorised third party (either within or outwith the council). All such information should be deleted immediately from the e-mail system and stored in the council's EDRM system or other identified secure location.

When using the Internet, social media and email, employees must ensure that they comply with Data Protection requirements and the council's IT Information Security Policy. Should any doubt arise on an issue that may have Data Protection Act implications, employees should contact their line manager or their local Information Liaison Officer for advice.

15. RESPONSIBILITIES

Depute Chief Executives and Heads of Service

Depute Chief Executives and Heads of Service are responsible for:

- ensuring that this policy is communicated to all employees;
- ensuring that use of the council's systems is monitored and standards of operation are consistently enforced in line with the terms of this policy;
- applying higher level access for staff where it is appropriate for business purposes

Service Managers

Service Managers are responsible for:

- determining, on the basis of business needs, those staff who require access to internet, social media and e-mail facilities to assist them in the performance of their duties;
- keeping authorised use/access under general review;
- approving the setting up of internet and social media sites for business purposes and monitoring the content of such sites within their service.

Line Managers

Line Managers are responsible for:

- ensuring that authorised users are given appropriate training and are fully briefed in the legitimate and lawful use of the systems in accordance with the standards set down in this policy;
- ensuring that all employees are made aware of the possible disciplinary and/or legal consequences of any breach of this policy and any associated procedures or codes of practice;
- investigate and act upon any concern regarding their staff's personal use of the systems to ensure that it complies with the terms of this policy;
- complying with council procedures for removing or amending the access rights of their staff who change jobs or leave the council;

Employees

All employees have a responsibility to:

- ensure that their use of Internet, social media and e-mail complies with IT guidelines relating to housekeeping and effective use of the councils systems;
- comply with the terms of this policy in relation to the legitimate, responsible and lawful use of the Internet, social media and email;
- manage the security of their own computers and the other standards of security in accordance with the council's Data Protection and Information Security Procedures;
- restrict personal use of the councils Internet, social media and e-mail facilities within the limits and conditions set out within this policy;
- adhere to guidelines for private use of the internet, social media and email and avoid prohibited activities;
- report suspected cases of misuse/breach of this policy to their line manager.

IT Services

IT Services are responsible for:

- maintaining all central e-mail and Internet facilities such as servers, software and network facilities;
- maintaining Internet network security, user accounts and filtered user access, and for monitoring and reporting on user access logs;
- reviewing the technical, operational and security aspects of this policy, in consultation with Service Units;
- issuing procedural guidance and codes of practice in support of this policy;
- carrying out periodic or sample checks to ensure that only authorised users have access to internal systems.

Corporate Communications

Corporate Communications are responsible for:

- supporting officers in making effective use of social media for approved council business.

16. REVIEW

This policy will be reviewed in consultation with the trade unions in the light of technological and legislative developments.

Appendix 1

POLICY ON USE OF INTERNET, SOCIAL MEDIA AND E-MAIL SYSTEMS

PROHIBITED ACTIVITIES

The following activities are expressly prohibited. Engaging in such activities may result in disciplinary action being taken against the individuals concerned, up to and including dismissal in accordance with the terms of the council's Disciplinary Code. The following list of activities is not exhaustive.

Employees using the Internet, social media and email for business, personal or private purposes must not:

Communication

- communicate or distribute libellous or defamatory material about any individual, firm, body or organisation, including the council;
- claim to represent the views of the council unless authorised to do so; only those employees who are authorised to communicate with the media may do so;
- transmit confidential or sensitive information relating to individuals or any aspect of the council's business over the internet, social media sites or via e-mail (other than by council approved, secure systems for external e-mail);
- publish material or a comment that could undermine public confidence in the council or misrepresent the council and its services
- manipulate dialogue or attempt to control people's points of view
- post derogatory comments about the Council, working for the Council or decisions made by the Council
- post expressions of personal anger or abuse against another employee
- publish untrue statements about another person which could damage their reputation or working relationships
- post comments to newsgroups or chat rooms on behalf of the council unless authorised to do so;

Inappropriate Behaviour

- knowingly accessing or attempting to access inappropriate Internet sites, download, store or circulate material which is illegal or inappropriate to the workplace. Inappropriate in this context includes sites or material which are for example, pornographic, racist, or sectarian, involve illegal activity, or other actions that contravene the council's disciplinary code or breaches general standards of conduct set by the council;
- send inappropriate messages/create posts which breach the standards and values set out within the council's Policies on Equal Employment Opportunities and Bullying & Harassment or which are otherwise abusive, threatening or provocative;

Legislation

- download, possess, distribute or copy works (e.g. document, photograph, piece of music or video) without the consent of the copyright owner;
- disclose personal data or information about any individual/colleague/service user which could be in breach of the Data Protection Act 2008;
- breach of any other relevant legislative requirement as specified within the council's Information Security Policy.

Security

- gain or attempt to gain, access to those parts of the council's network for which authorisation has not been granted, or to do so with the intention of damaging or disrupting the system, altering its normal performance or causing it to malfunction;
- falsify their e-mail address or otherwise generate messages in a manner which would make them appear to have come from someone else;
- breach the council's password security arrangements;
- intentionally access or transmit, information about or software designed for breaching security controls or creating computer viruses;
- give out personal details of employee's/clients like home addresses and phone numbers without checking whether the person requesting the information is entitled to receive it.

General

- purchase goods or services, or conduct other transactions over the Internet in the council's name without proper authorisation in accordance with relevant council procedures in force at the time e.g. rules governing e-procurement;
- use the council's systems for political party activity;
- use the council's systems for conducting a private or commercial business undertaking;
- use the council's Internet system for the purpose of online gambling or e-auctions (eg. Online Bingo, E-Bay);
- subscribe or register with personal newsgroups, shopping or social media sites with council accounts or email addresses;
- download software or accept cookies associated with personal online transactions e.g. ITunes, Napster, Amazon wish list etc.;
- participate in any activity that could cause congestion and disruption of network systems. This includes sending and forwarding unsolicited or inappropriate e-mail (known as 'spam') to groups or mailing lists, participating in chain or pyramid letters or similar schemes or making other excessive use of unsolicited e-mail;
- use the council's Internet for on-line game playing, chat lines or instant messaging (e.g. ICQ, AOL, Yahoo, MSN, Skype etc).
- post videos or pictures of others without their permission
- copy, download, transmit or alter pictures of others on the online staff directory.
- communicate with clients, pupils or service users as friends on Social Networking sites thereby potentially compromising or breaching professional standards of conduct
- Use the council's logo on personal web pages or social media sites.