KEY EMPLOYMENT POLICIES

EMPLOYEE INFORMATION BRIEFING SCRIPT

ISSUE 16: OCTOBER 2017

☐ NEW POLICY ☐ POLICY REVIEW ☑ REGULAR REMINDER

INTERNET, SOCIAL MEDIA & E-MAIL POLICY AND CYBER SECURITY

POLICY OVERVIEW

This policy sets out the council's corporate standards for the use of internet, social media and email by employees in the course of their work. A key aim is to ensure that those systems are used effectively and responsibly and in accordance with approved operational and security standards.

In addition, the policy outlines the responsibility of employees to ensure that their private use of internet, social media and email 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. The policy provides a list of prohibited activities that employees are encouraged to review in order to ensure their use of the internet, social media and email is compliant with the expected standards.

KEY INFORMATION FOR EMPLOYEES

- You must comply with council policy when using the Internet, social media and email for council business and personal purposes both **within and out with** the workplace.
- You are encouraged not to comment on your work or make reference to the council on external web pages such as Face Book. If you choose to do so, you must make it clear that you are not commenting in an official capacity as an employee and that the views expressed are your own and do not necessarily reflect the views of the council.
- Should you become aware of negative or disparaging remarks about the Council or its services, you should not respond but instead advise your line manager.
- You must never communicate or disclose information online in breach of the council's Data Protection Policy or Information Security Policy or take up positions on issues that are counter to the council's interests.
- You are reminded that if you wish to raise issues in relation to your employment with the council, you should not do so via social media but should direct such matters through the appropriate internal procedures such as the council's Procedures for Hearing Employee Grievances or through the Whistle Blowing procedure.
- Use of the Internet, Social Media or E-Mail in a manner that harasses, bullies, intimidates, threatens or demeans another council employee whether within or out with work breaches the council's Bullying and harassment Policy and Procedure, Policy on Equality in Employment and Service Provision and the Disciplinary Code

- You must report to your line manager, any instances of information being posted by another council employee on websites or social media sites that could be considered offensive, libellous, or potentially harmful to other employees, pupils, clients, community groups and service users of the council.
- Breaches of the council's Internet Social Media and Email Policy including those matters already referred to above will be investigated under the council's Disciplinary Procedures.
- Disciplinary investigations may extend to improper private use of the internet, social media and email where the action is considered to breach council policy and in certain extreme circumstances it may be deemed unlawful and the council will make appropriate referral to the Police.

Cyber Security

- You may be targeted with emails or internet links intended to help criminals penetrate council networks. Cyber-attacks can cause substantial downtime, loss and damage to council data which can take considerable time and money to recover lost information, recover systems and replace IT equipment.
- It is essential that you complete the Cyber Security online training module to gain a understanding of 'phishing' and 'ransomware', how to identify them and what to do if you come across suspicious emails or bogus websites.

Cyber Security Do's and Don'ts:

- ✓ Do check the legitimacy of suspicious emails where you know the sender
- ✓ Do allow security patching updates on your PC/laptop and comply with all requests to shut-down or reboot.
- ✓ Do ensure that you save your files in appropriate systems such as EDRMS.
- ✓ Do report all suspicious emails to the IT service desk immediately.
- × Don't open email from unknown sources or email addresses.
- × Don't respond to, click on links or open attachments on suspicious emails.
- × Don't save any critical files on your PC as they may not be recoverable.

ROLL OUT ARRANGEMENTS

- Services should ensure that records are kept of the date that employee briefings were conducted and the employees who attended. Those records may be subject to internal audit at any given time to ensure that council employment policies are being properly disseminated throughout services.
- Employees should be encouraged to read the full Internet, Social Media and E-Mail Policy available at http://www.westlothian.gov.uk/article/2200/Policies-Procedures-and-Guidance and accessible from work or home.

HR Policy and Advice
October 2017