

---

# CLYDE VALLEY GROUP

---

## **Staff Social Media Policy**

**Policy Number G27**

---

<b>Prepared By</b>	HR & Corporate Services
<b>Policy Created</b>	Staff Social Media
<b>Effective Date</b>	March 2020
<b>Review Date</b>	March 2021
<b>Posted on Website</b>	Yes

If you need this publication in larger print, audio form, Braille, or in another language, please contact our office and we will try to help you.

## **1. Introduction**

1.1 The purpose of this document is to set out the policy for staff use of social media when representing Clyde Valley group (CVG)

1.2 The Policy should be read in conjunction with the:

- Employee Code of Conduct
- Customer Service Standards

## **2. Background**

2.1 Social media has opened up new ways to communicate directly and engage with our customers. The significance and importance of social media for CVG has never been greater as it plays an increasing role in everyday life.

2.2 The content and communication on our social media channels supports CVG to deliver an online service to customers.

2.3 Currently CVG has an online presence on the following channels: Twitter, LinkedIn and YouTube.

## **3. Aims and Objectives**

3.1 The objectives of this policy are to:

- Establish a framework for providing access to CVG social media;
- Identify and ensure compliance with existing policies and procedures;
- Provide direction and guidance to staff regarding the use of social media generally.

## **4. Scope**

4.1 This Policy has been written to encourage the use and promotion of social media by CVG and to protect employees from its misuse.

4.2 While individuals not employed by the Association will not be subject to the disciplinary provisions relevant to employees ([see 9 below](#)), the remaining sanctions in respect of the misuse of social media will apply to all users (see Expected Behaviours Policy).

## **5. Definitions**

5.1 For the purposes of these guidelines, 'social media' is any type of interactive online media that allows parties to communicate instantly with each other or to share data in a public forum. This includes email, online social forums, blogs, video and image-sharing websites and similar facilities.

5.2 Employees should be aware that there are many more examples of social media than can be listed here and this is a constantly evolving form of communication. Employees should follow these guidelines in relation to any social media they use.

## **6. Legal and regulatory framework**

6.1 The use of the CVG's social media is regulated by Scottish, United Kingdom and EU legislation. Whilst the Human Rights Act 1998 protects freedom of expression and the right to privacy, these considerations are balanced against the need to ensure correct and lawful use of social media and the protection of business and other important interests. The legislation relevant to this policy includes, but is not restricted to, the following:

- General Data Protection Regulation (GDPR) 2018
- Human Rights Act 1998
- Copyright, Designs and Patents Act 1988 (CDPA)
- Computer Misuse Act 1990
- Regulation of Investigatory Powers Act 2000
- Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000
- Offensive Behaviour at Football and Threatening Communications (Scotland) Act 2012.

6.2 Other relevant guidance and information includes:

- The Information Commissioner's Data Protection Code: Employment Practices;
- Guidance published by the Information Commission from time to time;

6.3 Activity by any member of staff on social media must conform to CVG's personal and professional controls including:

- Contract of Employment
- Employee Code of Conduct
- Customer Service Standards
- Expected Behaviours Policy.

## **7. Responsibilities**

### **7.1 Executive Team**

All members of CVG's Executive Team have a responsibility to ensure that this policy document and any associated guidelines for use of social media resources accurately reflect the values, aims and objectives of CVG.

### **7.2 Leadership Team**

Managers should ensure their staff are aware of and comply with CVG's policies, procedures and guidelines for social media use.

### **7.3 Employees**

All employees should ensure that they are aware of and comply with CVG's procedures, policy and practices for social media use especially those procedures in relation to their personal accounts.

## **8. Social Media Use at Work**

8.1 Given the increasing use of social media as a key communication tool, staff can access social media during working hours and are encouraged to keep up to date with content shared by CVG accounts. However all employees must comply with this Policy.

8.2 When accessing social media for work purposes, employees can:

- Visit CVG's social media pages (e.g. Facebook, Twitter) and view video content on YouTube. Staff can follow CVG on Twitter or like our Facebook account from their personal accounts however they must ensure that their privacy settings are in place so that customers cannot see their personal information.

8.3 When accessing social media for work purposes, employees should not:

- Upload, download, create, send, receive, willingly distribute, access or store any material (text, images or any other material) that is: defamatory, offensive, obscene or threatening; racially, religiously or sexually discriminatory; indecent, abusive or likely to cause offence; incites, threatens or depicts violence; describes techniques for criminal or terrorist acts; contains any form of illegal content.
- Engage in any activities which could cause congestion and disruption of CVG's social media resources or affect its reputation in a negative way. This would include sending and forwarding unsolicited, irrelevant or inappropriate messages to groups or mailing lists, participating in chain or pyramid letters or similar schemes or making other excessive use of unsolicited messages. This list is not exhaustive.
- Break through security controls, whether on the CVG's social media accounts or on any other social media accounts.
- Access to CVG's social media resources that are not intended for them, even if it is not protected by security controls, or doing anything that will adversely affect the ability of others to access social media resources which they are entitled to access.
- Access or transmit information about, or software designed for, breaching security controls or creating computer viruses.

## **9. Accessing Personal Accounts**

9.1 CVG understands that employees may want to use their work devices, such as desktop computers, mobile phones, laptops and tablets, to access non-work related or personal social media accounts while they are at work during their allocated break times. Employees must limit use of personal accounts so as not to interfere with their working day and use must be limited to allocated break times.

## **10. Personal Use of Social Media**

10.1 Staff should check their own privacy settings to ensure that their own posts and personal information do not cause reputational damage to CVG customers or themselves. Preferably, on Facebook and Twitter staff should not state they work at CVG unless they are considered to have a specialist role. In this instance, it must be clearly stated that 'views are your own.'

- 10.2 Staff are encouraged to share content posted by CVG social media accounts however they should not link to, talk to, comment or post messages or images either to or about customers on their personal social media accounts. Posting images of our customers, even if they are in background, is not permitted.
- 10.3 Staff should not use their personal profiles to comment on posts, general or negative, by external stakeholders such tenants or community members that are in relation to CVG.
- 10.4 If there is any doubt about what is an acceptable posting or comment on your personal account(s), please contact a member of the Corporate Services Team.

## **11. Responses to breach of policy**

- 11.1 This Policy is non-contractual and CVG may change it from time to time. When changes are made to this Policy, Human Resources will provide users with an updated form to sign. The new form will replace any previously signed forms.
- 11.2 Staff should be aware that breach of this policy may lead to disciplinary action.

## **12. Review**

- 12.1 The fast changing nature of information technology, particularly in relation to electronic communication incorporating aspects such as social media, means that the policy and procedures will be reviewed at least every two years and sooner if considered appropriate.