Southside
HOUSING ASSOCIATION

Policy on Social Media

Issued: November 2015

Review Date: November 2018

1.0 INTRODUCTION

1.1 Southside Housing Association (SHA) recognises the potential of social media as a business tool. As information and communication technology continues to move forward, so too do the tools that enable us to communicate with and unite people.

1.2 'Social Media' is the term used for online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests. It involves building online communities or networks, which encourages participation, dialogue and involvement.

1.3 Types of social media may include blogs; wikis; social networks; social bookmarking, forums; image, audio and video sharing sites; and other content sharing communities. Typical social media sites may include Facebook, Twitter, Google +, Pinterest, Youtube, Vimeo, Vine, Keek, Flickr, Audioboo, Soundcloud, Mixcloud, Tumblr and other blogging tools. The format and levels of interaction vary greatly from one to another.

1.4 For social media to work effectively it is vital that it is used as part of the overall communication mix; to provide up to date information about the Association, our Subsidiaries, the services we provide and our engagement activities. Social media also provides the opportunity of being able to connect with the community, listen to what people are saying and engage with them on an equal footing; focusing on two way communications.

1.5 It can empower local residents to have a voice about their needs and influence decision making, building trust and stronger communities.

1.6 We need to ensure that our use of social media does not expose the Association to security risk or reputational damage and this policy and appended staff guidance sets out how we will manage and regulate this.

2.0 AIM OF POLICY

2.1 Social media offers the potential for building relationships and improving the services that we provide. This Policy will clearly set out how social media can be managed effectively and how any risks or pitfalls can be avoided or mitigated.

2.2 The aim of this Policy is to:

- safeguard the Association and staff by identifying who is permitted to represent us on social media sites and to provide guidance to staff members who have their own personal social networking sites;
- encourage good practice in using social media and ensure that users operate within existing policies, guidelines and relevant legislation;

- support our Digital Inclusion agenda;
- promote the effective and innovative use of social media as part of the Association's activities. Where appropriate, the use of social media will become an integrated part of communications and engagement plans for projects, campaigns and consultations;
- encourage and promote engagement with individuals and local communities;
- ensure that the Association's information remains secure and is not compromised through the use of social media; and
- ensure that the Association's reputation is not damaged or adversely affected.

3.0 SCOPE

3.1 This Policy applies to all staff, volunteers and other workers (including placements and agency workers and secondees).

3.2 A core group of named staff will form the 'Social Media Implementation and Development Group' (SMIDG) and manage all social media content produced on behalf of the Association. This is to ensure the content is consistent with our core messages and values and that it does not conflict with information already being communicated through more traditional methods.

3.3 Specific guidelines for all staff have been developed on the use of social media tools, including personal use. These guidelines have been designed for staff using social media for business and personal purposes and are attached to this Policy (Appendix 1).

3.4 This Policy should be read in conjunction with the following policies/documents within the Association:

- Complaints Policy
- Code of Conduct
- Openness and Confidentiality Policy
- Data Protection Policy
- Dignity at Work Policy
- Information Technology Policy and Procedures
- Accidents, Incidents and Near Misses Procedures.

3.5 This Policy provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise the Association's 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 Association or its business, nor be damaging to our reputation and credibility or otherwise violate our policies.

4.0 BENEFITS

4.1 The benefits of using social media can include:

- Adding a new dimension to the Association's communication and engagement strategies with a channel that is immediate, direct and allows fast dissemination of information – particularly useful during any kind of disruption to services;
- attracting and engaging with tenants, customers and stakeholders by bringing messages to life with video/audio/images;
- offering another channel to help understand and respond to (where appropriate) customers' complaints, compliments or problems;
- communicating key messages in a cost-effective way;
- providing another option for tenants and customers to contact us when and through a medium that suits them, including rent payments;
- reaching out to a wider UK social housing audience – sharing our success stories;
- providing an opportunity to build online communities which are location specific (areas, even streets), so that we can share information and engage with specific geographic communities;
- increasing positivity around our brand as 'followers' or 'friends' become brand advocates;
- increasing access to communities, for example young people;
- providing opportunities for other stakeholders (e.g. local organisations) to engage with us; and
- helping to deliver our Digital Inclusion agenda.

5.0 RISKS

5.1 As with any online activity there are risks associated with it. The following risks should be considered:

- Improper/incorrect posting of information on internal and external social media sites (including on an individual's own time);
- increased risk of viruses/malware (malicious software);
- risk to staff where they identify themselves as working for the Association;
- disclosure (intentionally or unintentionally) of confidential information;
- social engineering attacks (this is the act of manipulating people into disclosing confidential material or carrying out certain actions. Social engineering is often conducted by individuals fraudulently claiming to be a business or client);
- out of date information which can be misleading;
- civil or criminal action relating to breaches of legislation; and
- breach of Safeguarding

5.2 The following will be applied to help manage and reduce the risks outlined above:

- Identification of a Lead Officer with overall responsibility for the Association's social media presence, who will be accountable to the Director;
- the 'Social Media Implementation and Development Group' (SMIDG) will be established to regularly monitor and develop the Association's social media presence;
- safeguarding steps and settings will be applied to all social media sites to ensure all content is approved by an identified staff member before being published;
- provision of in-depth training for staff within the SMID group;
- provision of awareness raising training for all staff and volunteers to raise awareness of their personal and professional social media responsibilities;
- implementation of a quality assessment framework, which the SMID group will have responsibility for monitoring;
- sufficient antivirus/anti-malware protection to render risk minimal and acceptable; and
- guidelines to safeguard staff and volunteers on the use of social networking sites are included as part of the Social Media Policy.

6.0 RESPONSIBILITIES OF STAFF AND VOLUNTEERS

6.1 The following guidelines apply to online participation by staff and volunteers and set out the standards of behaviour expected as a SHA representative.

- Be aware of and recognise your responsibilities identified within this Policy;
- remember that you are personally responsible for the content you publish on any form of social media;
- be aware of safeguarding issues, as social media sites are often misused and safeguarding is everyone's business – if you have any concerns about other site users, you have a responsibility to report these;
- never give out personal details such as home address and telephone numbers. Ensure that you handle any personal or sensitive information in line with data protection policies/guidance;
- respect copyright, fair-use and financial disclosure laws;
- 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 sought if you wish to publish or report on meetings or discussions that are meant to be private. Individuals must not be identified without their approval;
- don't use insulting, offensive or racist language or engage in any conduct that would not be acceptable in the workplace. Show consideration for others' privacy and for topics that may be considered objectionable or inflammatory – such as politics or religion and in relation to staff the Dignity at Work Policy applies; and
- don't download any software, shareware or freeware from any social media site.

6.2 Further guidelines have been appended to this policy.

7.0 RESPONSIBILITIES OF STAFF

7.1 Authorised staff responsible for the Association's social media must be aware of and comply with the Association's Guidelines (within appendix 1) and Employees' Code of Conduct.

7.2 When representing the Association on social media staff must identify themselves as being part of the Association and only use email addresses provided by the Association and not personal ones.

7.3 If a member of staff receives any threats, abuse or harassment from members of the public through their use of social media they must report such incidents using the Association's Accident, Incident and Near Miss Reporting procedures.

8.0 VOLUNTEERS

8.1 Volunteers should ensure that they are familiar with the guidance set out in this Policy and that their use of social media does not put the Association's information and security systems at risk, or damage our reputation.

8.2 Volunteers should also be familiar with their Code of Conduct, which outlines key information and guidance on best practice issues such as information handling and security.

9.0 PERSONAL USE

9.1 This policy refers to the business use of social media. Staff who have been granted access to social media sites should not use the Association's social media sites for personal reasons.

9.2 Staff should be aware that Staff Code of Conduct covers the issue of fidelity and information disclosure and should bear this in mind when using social media (in a personal capacity) out-with work. Staff should be aware that any reports of inappropriate activity, linking them to SHA will be investigated.

9.3 Appendix 1 outlines the legal considerations which arise through employees' use of social media and it is important that staff refer to and familiarise themselves with this guidance. Failure to comply with the guidelines could result in disciplinary action being taken.

10.0 RESPONDING TO CUSTOMERS

10.1 Where possible social media sites will be set up to minimise the opportunity for customers to publicly use offensive language, including swearing or sectarian, sexist or racist comments.

For example, Facebook will be set up whereby all posts will be reviewed by the lead group for social media before being publicised. Alongside this a section containing 'house rules' will be developed to ensure those posting are clear about what is acceptable and not acceptable.

10.2 The Association will not respond to posts on social media which contain offensive language, for example swearing or sectarian, sexist or racist comments. These posts will be removed and will not be 'approved' for public viewing.

10.3 The Association's social media sites will not be considered formal routes for complaint and all customers wishing to complain will be made aware of the Association's processes. Complaints will be dealt with in line with the Association's Complaints Policy.

11.0 MONITORING

11.1 The contents of our IT resources and communications systems are the Association's property. Therefore, staff should have no expectation of privacy in any messages, files, data, document, social media post conversation or message, or any other kind of information or communications transmitted to, received or printed from, or stored or recorded on our electronic information and communications systems.

11.2 In accordance with agreed processes for monitoring IT usage by individual staff members, we reserve the right to monitor, intercept and review, without further notice, staff activities using our IT resources and communications systems, including but not limited to social media postings and activities, to ensure that our rules are being complied with and for legitimate business purposes and you consent to such monitoring by your acknowledgement of this Policy and your use of such resources and systems. This might include, without limitation, the monitoring, interception, accessing, recording, disclosing, inspecting, reviewing, retrieving and printing of transactions, messages, communications, postings, log-ins, recordings and other network monitoring technologies.

12.0 SUSTAINABILITY IMPLICATIONS

12.1 This Policy supports our commitment to digital inclusion. The regulated use of social media has the potential to make a positive impact on communities and social wellbeing. By establishing greater links with members of the public, community groups, partners and stakeholders, through social networking, there is scope for more open communication and the increased ability to share information and to improve service delivery.

13.0 BREACHES OF POLICY

13.1 Any breaches of this Policy may lead to social media access being withdrawn (on a professional basis) and disciplinary action being taken. Serious breaches of this Policy by staff will amount to gross misconduct and may result in dismissal.

13.2 Other violations of this Policy, such as breaching the Data Protection Act, could lead to fines being issued and possible criminal or civil action being taken against the Association or the individual/s involved.

14.0 LEGAL AND REGULATORY FRAMEWORK

14.1 The following legal documents are relevant to this Policy:

- Data Protection Act 1998
- Freedom of information Act 2000
- Human Rights Act 1998
- Computer Misuse Act 1990
- Copyright, Designs and Patent Act 1998
- The Telecommunications Regulations 2000
- Regulation of Investigatory Powers Act 2000

14.2 Anyone who uses social media and holds, shares, refers to or uses i.e. processes personal information must comply with the eight principles of the Data Protection Act 1998, as must the Association. This Act ensures personal information is:

- fairly and lawfully processed
- processed for limited purposes
- adequate, relevant and not excessive
- accurate and up to date
- not kept longer than is necessary
- processed in line with the individuals rights
- secure
- not transferred to other countries without adequate protection.

14.3 Copyright protects the right of the author to control the production and use of copyright material. Authorised staff using social media should do so without infringing the copyright of others, including the Association's own copyrights and brands. In some situations it might be possible to use copyright material where only a short excerpt of someone else's work is used and the author or source of the material is linked.

14.4 Effectively managing and protecting the Association's confidential information and 'trade secrets' for example business performance, is critical and the responsibility of all Association staff, contractors and partners. Confidential information and trade secrets are part of our assets.

14.5 Failure to effectively manage and protect our own and our contractors', partners' and suppliers' confidential information may result in customer complaints, regulatory enforcement action or fines, breach of contract, damage to business relations and damage to the Association's reputation.
Failure to prevent disclosure or reference to court proceedings, including pending proceedings, may prejudice those proceedings.

14.7 Effective management of the physical security of the Association's intellectual property is critical and the responsibility of all staff, volunteers, contractors and partners. The sharing of this type of information on social media sites may compromise the security of a building or complex.

15.0 POLICY REVIEW

15.1 This policy is subject to regular review to ensure it is up to date with developing technology and online social tools. A review will also be necessary following changes to legal, regulatory or best practice. As a minimum, it will be reviewed every three years. Reviews will be approved by the Senior Management Committee.

APPENDIX 1: GUIDELINES FOR STAFF AND VOLUNTEERS

We recognise that the internet provides opportunities to participate in interactive discussions and share information on particular topics using a wide variety of social media, such as Facebook, Twitter, blogs and wikis. However, employees' and volunteer use of social media can pose risks to our confidential information, our reputation and it can also jeopardise our compliance with legal obligations.

To minimise risks we expect all staff and volunteers to adhere to these guidelines as well as the main content of the Social Media Policy.

This guidance is for all staff and volunteers using social media, including Facebook, Twitter, all other social media networking. This guidance also covers all other internet postings, including blogs.

This guidance applies to the use of social media for business and personal purposes, whether during office hours or otherwise and regardless of whether social media is accessed using the Association's IT facilities or personal equipment belonging to staff or volunteers.

BE RESPONSIBLE FOR WHAT YOU WRITE

Exercise good judgment and common sense when making comments online.
It's okay to have opinions but don't do so in a way that may not be appreciated by your audience or may damage the Association's reputation. If you are in doubt about whether or not you should post a comment, this will usually mean that the post or comment is not appropriate.

To give you some guidance on how to exercise good judgment, here are some examples of what not to do:

Staff and volunteers should never post any disparaging or defamatory statements about:

- the organisation;
- our customers;
- our suppliers and business partners; and/or
- our stakeholders and other affiliates.

Staff and volunteers should also avoid any social media communications that might be misconstrued in a way that could damage the Association's reputation, even indirectly.

Do not post anything that your colleagues or customers would find offensive, including discriminatory comments, insults or obscenity. This means always be, truthful and respect the other individual(s). Never embarrass or make fun of others online. Workplace bullying includes comments made online, including within your personal social network profiles or out of office hours.

Refrain from making any comments that could be interpreted as demeaning, inflammatory or judgmental, or likely to cause injury or upset to another person. You should never post anything that relates to our tenants, customers, business partners, suppliers or stakeholders, nor should you make any comments which these people might find offensive or inappropriate or which might damage their reputation.

NEVER REVEAL TOO MUCH INFORMATION

Never reveal confidential or sensitive information about yourself, your colleagues or the Association to anyone online. Don't re-post internal communications as these are not for public consumption. All employees within the Association already have a confidentiality clause included within their Contract of Employment and employees should be mindful of this when using social media.

REMEMBER THAT CYBERSPACE LINKS YOUR PROFESSIONAL AND PRIVATE LIVES

If you have personal social media sites such as Facebook and Twitter and receive friend requests from people who you know are SHA customers, consider whether you know them well enough to accept them as friends.

You should also consider whether you need to tell people where you work. If you decide to do so friends and customers who find your private Facebook page and personal Twitter account, may draw their own conclusions. Be cautious before putting anything 'out there' as it may damage our reputation or otherwise breach these guidelines.

If you do identify where you work and make comments on the Association's business we would recommend that you use a disclaimer such as "The views expressed on this site are my own and in no way reflect the views of Southside Housing Association". However, this does not itself exempt staff and volunteers from personal responsibility. You should not use our organisation's logos, brand names, slogans or other trademarks – this is all property of the Association, and should not be used by staff for personal social media profiles.

ENGAGE HONESTLY AND TRUTHFULLY

If you cannot help someone directly on social media send them to the appropriate department, person or social media channel.

Follow up personally or make sure a colleague does so. Make sure that you provide updates to the customer as/when required. Aim to resolve the majority of enquiries within 5 working days but let the customer know if this is not going to be possible. In today's virtual world time is of the essence. The Association's social media sites will not be recognised formal complaint routes and thus customers should be redirected to the official complaints route when required.

The Association will adopt a “respond once, then step away” approach to avoid getting drawn into back and forth comments with customers. Where appropriate customers will be encouraged to take issues/comments into a private conversation via email/private message or telephone.

Only authorised members of staff are allowed to post comments using the organisation’s social media profiles. These staff members must follow these guidelines and, in any event, receive authorisation from named lead officer before posting content on the Association’s behalf.

VERIFY YOUR PRIVACY AND SECURITY SETTINGS

How much, or how little, information you reveal – such as email or phone number – should be set in your security options or privacy settings (e.g. what information is visible to anyone).

Consider whether you really need to tell people where you work. If you make inappropriate comments or share racist /sectarian /offensive /obscene /sexually suggestive/ harassing/sexist /pornographic/ discriminatory material that a tenant or other member of staff sees, this may lead to a complaint which may, in turn, lead to you being disciplined.

Before you post any images or videos online on any internal Association social media site, staff should be mindful of this guidance and ensure compliance.

WATCH THE CLOCK WHEN USING SOCIAL NETWORKS

Access to social media sites is restricted on the Association’s IT systems. However many staff will be able to access these sites using their personal mobile phones. Visiting your personal social media sites takes time away from getting tasks done for which you get paid; accordingly, use your time wisely while at work and make your social media engagement beneficial to the company. Access to personal sites, regardless of how you access them, should be limited to break/lunch time. Please do not let such usage interfere with maintaining your high performance. When using the Association’s social media sites make sure you maintain a good balance between this and the rest of your work. This applies to phones, tablets and PCs.

Staff must only access the Association’s social media profiles using the Association’s IT devices. Staff must not log in to Association profiles on devices that are simultaneously logged in to other profiles on the same social media platform. This reduces the risk of staff accidentally posting information/comments when logged into the wrong profile.

Remember that you are not allowed to use the Association’s systems or equipment to access external social media sites such as Facebook and Twitter, unless you have specific authorisation to do so in order to perform your duties.

DISCIPLINARY ACTION

All staff and volunteers are expected to comply with the terms of this policy. Disciplinary action (up to and including dismissal) will be taken against any employees or volunteers who fail to do so, in line with the appropriate policy.

You should be aware that disciplinary action may be taken regardless of whether the breach of these guidelines is committed during working hours, and regardless of whether you use personal equipment to access the relevant sites. Any member of staff suspected of committing a breach of these guidelines or the Social Media Policy will be required to cooperate with our investigations.

Staff and volunteers may also be required to remove internet postings which are deemed to constitute a breach of these guidelines or the Social Media Policy. Failure to comply with such a request may in itself result in disciplinary action.

Employees and volunteers may face disciplinary action where, following appropriate investigation, they are found to have:

(a) Posted comments and/or images on the Association's/personal social media sites that others have found to be offensive;
(b) been responsible for serious breaches of security or confidentiality, including misuse or disclosure of confidential information via social media;
(c) used the Association's/personal social media in a way that has brought the Association into disrepute;
(d) used the Association's/personal social media in a way that has offended or damaged the reputation of our tenants, customers, suppliers, business partners, stakeholders or other affiliates;
(e) deliberately misused the Association's property (including computer facilities e.g. e-mail, social media and internet);
(f) made negative comments about the Association's business activities or employees;
(g) breached any of the following policies or obligations through posting of content on social media:
    - our obligations to the Scottish Housing Regulator;
    - our Information Technology Policy and Procedure;
    - our confidentiality obligations to third parties;
    - our Dignity at Work Policy;
    - our Employee Code of Conduct;
    - our Equal Opportunities Policy; and
    - our Data Protection Policy.

This list is not exhaustive.

UNACCEPTABLE ACTIONS

If you are subject to threatening or inappropriate posts on social media from customers or colleagues you should immediately report this to you line manager or a senior member of staff. In addition you must complete the Accident, Incident and Near Miss form.

MONITORING OF SOCIAL MEDIA

The content of social media sites operated by the Association is monitored by the SMID group. This will contain a mix of staff from across the organisation. All users of our social media sites are subject to house rules which include removal of offensive or unacceptable posts. If you have any concerns regarding the posts on our social media sites talk to your manager or a member of the SMID group.

REMEMBER

- What you publish is searchable and will be public for a long time.
- What you write is your responsibility.
- If you have concerns about what has been posted on social media sites speak to your line manager.