SOCIAL MEDIA POLICY FOR MEMBERS AND OFFICERS

1. INTRODUCTION

1.1. Social Media includes the various online technology tools that enable people to communicate easily via the internet to share information and resources. Social media includes, but is not limited to, blogs; wikis; RSS feeds; social networking sites such as Facebook, LinkedIn and Twitter; photo sharing sites such as Flickr, Instagram and Snapchat; and video sharing sites such as YouTube.

1.2. The widespread availability and use of social networking applications brings opportunities for the Councils to better understand, engage and communicate with its customers, partner agencies and the communities it serves.

1.3. This Policy supports the Councils' stated purpose, ambition and values by enabling the organisation to make best use of these technologies and so improve the way it does business. It also sets out a behavioural framework for Officers and Members to ensure that the considerable benefits that accrue from using social media are adequately balanced against our legal responsibilities and the need to safeguard the Councils' image and reputation.

2. PURPOSE AND OBJECTIVES

2.1. The purpose of this policy is to:

- ensure Officers are aware of their responsibility to comply with good practice and the law for example in relation to data protection, confidentiality, libel, copyright, safeguarding of children and vulnerable adults, human rights, harassment and discrimination so that the Councils are not exposed to legal and governance risks;
- support safer working practice by setting standards of good practice and behaviour in the use of social media;
- ensure the reputation of the Councils and its Officers are not damaged;
- ensure children, young people and vulnerable adults are safeguarded by reducing the risk of positions of trust being abused or misused;
- minimise the risk of misplaced or malicious allegations being made against those who work with vulnerable groups;
- ensure users of social networking media are able to clearly identify where information provided via such applications is legitimately representative of the Councils;
- enable Officers to distinguish between the use of social media in their work and personal lives;
- ensure the use of social media is aligned to the Council's corporate communications approach.

3. OTHER CODES AND POLICIES

3.1. The Councils' Code of Conduct for Officers applies to all offline and online communications and includes the use of social media, and can in some circumstances apply to the use of social media in an Officer's personal life.

3.2. The Councils' Disciplinary Policy applies to online communications and includes the use of social media, and can in some circumstances apply to the use of social media in an Officer's personal life.

3.3. The Council's Code of Conduct for Elected Members applies to a Member's use of Social Media.

4. USE OF SOCIAL MEDIA BY ADUR & WORTHING COUNCIL OFFICERS

4.1. Social media is used to communicate news and updates from the Council and the wider community and residents. It is also now an important customer service tool. The two main channels used are Facebook and Twitter.

4.2. There is also a Council presence on Linkedin and Youtube.

4.3. The majority of public facing communication via the Councils' corporate social media channels should be either produced or approved by the Council's Communications Team.

4.4. Some individual Councils accounts or aspects of social media management, such as incoming customer enquiries, can be operated by other members of staff. However, this is only by prior approval of the Head of Communications and after full training delivered by the Communications Team is completed.

4.5. A Council service can request to create a public social media page by submitting a business case outlining how social media would benefit this service and how it will be maintained or managed. This should be submitted for review to the Head of Communications.

4.6. If approved, the social media pages will be set up in collaboration with the Communications Team and all design must be in line with the Councils' branding.

4.7. All new social media pages will be reviewed after a period of 4 months. Those sites which are not performing well or are not benefiting residents will be removed. Similarly, any unauthorised sites will be closed down. Contact the Head of Communications for more information.

4.8. Officers may be permitted to use a Council's Twitter account to represent their role within the local authority. These must:

- Be requested and approved by the Head of Communications;
- Be clearly identifiable as a corporate account using @nameAWC
- Include the relevant Adur/Worthing/Joint logo in the header or profile image

5. PERSONAL USE OF SOCIAL MEDIA - OFFICERS AND MEMBERS

5.1. Social Media is now part of everyday life and routine and the lines between personal/ professional use can become blurred.

5.2. Officers and Members must be aware that their actions online on their personal pages may have wider implications on their professional role and on the Councils' image/representation. Always bear your relevant Code of Conduct in mind when you post to social media.

5.3. In the event that an Officer/Member's online conduct impacted on the Councils this would become a matter of council concern and may result in investigation in accordance with the Council's Disciplinary Procedure.

5.4. All Officers and Members should familiarise themselves with the privacy settings of each social media platform they are using and ensure these are set up correctly. You should never include any personal information (DOB, phone number, address etc.) on your personal profile, nor should you share this with residents or third parties.

5.5. Never publish confidential information which you have received as part of your job. Nor should you use any such information for personal gain or pass it on to others who may use it in such a way.

5.6. Staff should be aware of not using personal online profiles to raise or discuss a complaint or grievance about the Council, your manager, colleagues etc. There are formal procedures in place for progressing these within the Council.

6. DATA PROTECTION AND SUBJECT ACCESS REQUESTS

6.1. As per section 5.5, to adhere to the latest data protection laws, i.e. (EU General Data Protection Regulation 2016/679 and Data Protection Act, 2018 you should never share any sensitive or personal information to social media about a colleague, Member or resident. Any instances of this will be investigated and may lead to disciplinary action.

6.2. Data protection law was introduced to respect an individual's fundamental right to privacy through the protection of their personal data. Personal data is identified as 'any information related to an identifiable individual'.

6.3. Observe the privacy notices of the social media platforms for which you sign up to and check the privacy settings to see who your posts are shared with.

6.4. Personal data collected outside of social media by AWC may only be shared on social media if such sharing was stated explicitly under the AWC privacy notice that was used to initially collect the data.

6.5. The sharing of 'special category' data, i.e. ethnicity, religious beliefs, trade union membership (refer to ICO website for full list) may only be shared on social media with the consent of the individual (data subject) and must be accurate at the time of posting.

6.6. The sharing of personal data on social media must be noted in the Register of Processing Activity (RoPA) for the respective service who collected the information in the first instance.

6.7. Members of the public can submit a Subject Access Request (SAR) via our corporate social media pages. The right of access, commonly referred to as subject access, gives individuals the right to obtain a copy of their personal data as well as other supplementary information.

6.8. More information about an SAR can be found here: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

6.9. Members of the public may also exercise their other rights, i.e. right to rectification, erasure, restrict processing, data portability, object and automated decision making including profiling via our corporate social media pages.

6.10. More information about other rights may be found here:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/

7. MEMBER CODE OF CONDUCT

7.1. Members should be very careful in respect of their actions on their personal pages as the Member Code of Conduct may apply to them when they are not expecting it.

7.2 Elected and Co-opted Members are bound by the provisions of their Code of Conduct for Members when they are conducting Council business or acting, claiming to act, or giving the impression of so acting, as a representative of the Council, or in their official capacity as a Councillor. However, the law has held that whether a Councillor uses a personal social media or email account or a Councillor one is not definitive, and neither is whether he/she signs off of refers to themselves as a Councillor or not (*MC v Standards Committee of LB of Richmond 2011*).

7.3 Most personal information collected for use by Councillors uses the 'Public Task' legal basis and any subsequent sharing or disclosure of personal information on social media satisfies that basis.

8. LINKED DOCUMENTS

8.1. There are a number of policies which should be considered in conjunction with this social media policy. These can all be found on the Councils' Intranet, or hard copies can be provided on request. These are:

- The Councils' IT Policy
- The Councils' Disciplinary Policy
- The Councils' Use of Social Media in Investigation Policy
- The Councils' Officer Code of Conduct (see intranet)
- The Adur District Council Members' Code of Conduct
- The Worthing Borough Council Members' Code of Conduct