Social Media Policy

Owner	**: Matt Woor** **: Senior Communications Officer** **(Digital and Social Media Specialist)**
Document ID	**:**
Version	**: 1.3**
Date	**: April 2021**

We will on request produce this Policy, or particular parts of it, in other languages and formats, in order that everyone can use and comment upon its content.

DOCUMENT CONTROL

Changes History

Issue No	Date	Amended By	Summary of Changes
Draft 0.1	15/07/2015	Matt Woor	Drafted Policy
1.0	01/10/2015	Matt Woor	Published Policy
1.0.1	11/05/2016	Matt Woor	Added section 8.1 FOI appendix
1.0.2	12/07/2016	Matt Woor	Added section 8.2 SFRS appendix
1.2.0	12/12/2016	Matt Woor	Policy reviewed and republished
1.2.1	09/10/2017	Matt Woor	Added section 8.3 Councillor appendix
1.2.2	01/05/2018	Matt Woor	Added GDPR paragraph (section 3.7)
1.3	01/04/2021	Matt Woor	RIPA additions.

Review and Approval

Role	Name	Approval Date
Senior Manager Customer Experience	Mark Burgess	12/08/2015
Policy Clearing House	Allison Coleman	25/08/2015
HR Policy Review	Jeanette Bray	14/09/2015
Customer Data and Insight Manager	Alastair McCartney	12/05/2016
Senior Manager Customer Experience	Mark Burgess	01/06/2016
Service Review and Improvement (Fire)	Deborah Godfrey	12/07/2016
Appendix review by Fire Unions	Fire Unions	08/11/2016
Senior Manager Customer Experience	Mark Burgess	12/12/2016
Monitoring Officer	Tim Ryder	09/10/2017
Senior Manager Customer Experience	Mark Burgess	12/10/2017
Information Policy and Compliance Manager	Adele Rhodes-Girling	30/04/2018
Head of Legal Services	Nigel Inniss	26/03/2021
Head of Customer and Online Services	Mark Burgess	07/04/2021

Authorisation

Role	Name	Approval Date
Head of Customer and Online Services	Mark Burgess	07/04/2021
Head of Communications and Marketing	Andrew St Ledger	07/04/2021

Review Period

Date Document to be Reviewed	By whom
01/04/2022	Matt Woor

Table of Contents

1   Introduction

Social media is the collective term for the current set of online tools, websites and interactive media that enable users to interact with each other in various ways, through sharing information, opinions, knowledge and interests in a variety of forms. Social media involves building online communities and/or networks which encourage participation or dialogue and involvement.

The number of different social media tools is vast, and growing every year, but some of the larger more recognised tools currently include:

- Facebook
- Twitter
- LinkedIn
- YouTube
- Instagram

There are detailed appendices as part of this policy which will look at these and other social media tools in more detail should you need more specific information.

For social media to work properly, to be effective it is vital that it is used in association with other more traditional communications and customer engagement channels. Relevant and up to date information about the council, its services and activities should be published on the corporate website or associated strategic websites and social media should signpost people to appropriate online content to best answer their query.

As a council we need to set out clear guidelines for staff on the use of social media to ensure that resources are used effectively to deliver good customer service and effective communications. We also need to be aware of the risks of using social media and set about exposing those risks and how users can mitigate those risks to protect the council and themselves against security or reputational damage. This policy will provide those guidelines.
Social media is fast changing, rapidly evolving and constantly expanding into new areas. This policy will try to keep pace with these changes both from a tool point of view but also from a service user perspective. The appendices of this policy will be constantly updated and will look to encompass changes in both.

1.1   Policy Statement

The purpose of this policy is to state the social media policy of Suffolk County Council (SCC). This includes the corporate use of social media, and provides guidance on the expected behaviours of users on these and other sites. It also outlines the governance process around how social media sites will be set up to promote council services or the delivery of services, and how social media can be managed in a safe and responsible way.

The aim of this policy is:

- To preserve and protect the reputation of SCC and its staff
- To support the development of SCC's social media channels to promote customer engagement, promotion of council services, share key messages, and improve digital based customer services
- To inform staff and other users about the acceptable use of social media in their professional capacity, ensuring the council is not brought into disrepute by affiliation with unsuitable sites or through comments posted onto public online forums.
- Provide awareness of the Social Media Single Access Platform (SMSAP) and why/where it is used.
- To support staff in the healthy use of social media.

What this policy does not aim to do is replace established HR and IT policies on information security, data protection, general staff behaviours or conduct.

1.2   How this policy is structured

This policy is one part of a wider library of information about the council's approach to social media. The strategy will deal with why the council wishes to engage with customers via social media, the perceived benefits/risks of this engagement and the corporate principles of engaging in this way. The policy will deal with how the council will manage and use social media as an everyday business as usual function, expected behaviours of staff and key officers, stakeholders and budgets. The directorate appendices will be written in conjunction with each directorate to provide specific social media guidance and direction for the various directorates – focusing on their target audiences, services and specialisations. This will allow council officers greater flexibility of how to use social media to maximise the benefits unique to them and their service area.
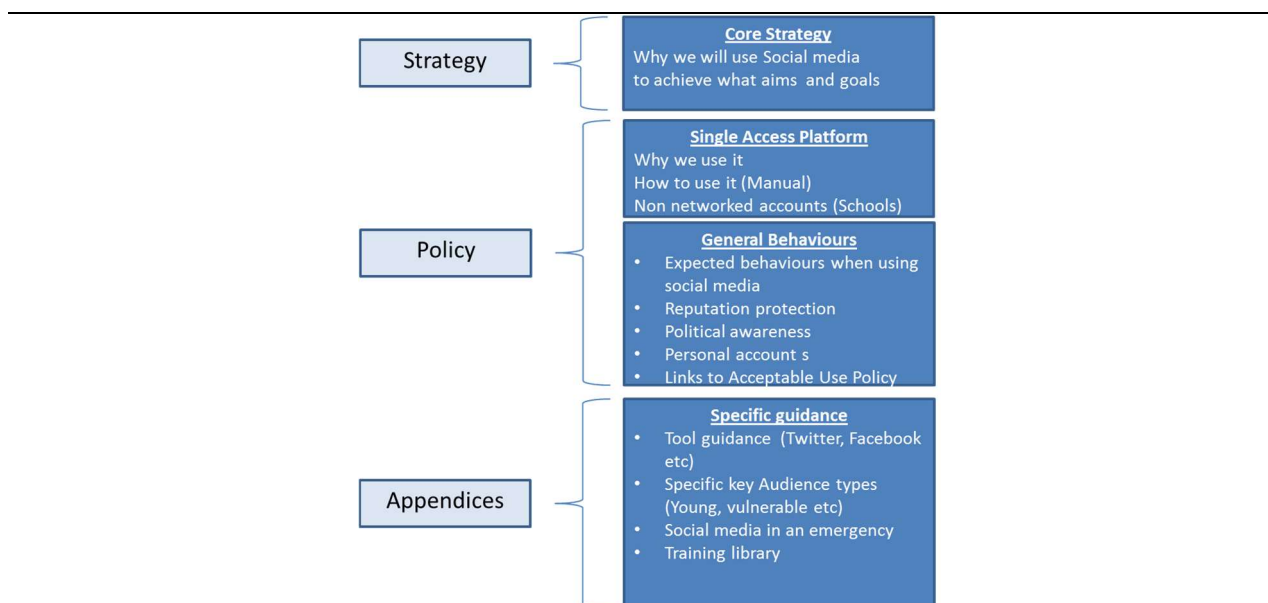
1.3 Scope

SCC accepts that social media can be beneficial to staff in performing their role to serve the people of Suffolk. Because of this the council has enabled access to the majority of social media tools via its corporate network making them accessible to all members of staff. This access is provided on the basis that staff act responsibly and adhere to the acceptable behaviour and other guidelines outlined in this policy and in supporting polices such as the Acceptable Use of IT policy.

This policy applies to the use of Social Media for which SCC is accountable and responsible. It is applicable to SCC Councillors, SCC employees, partners and agents who SCC employees have authorised to use Social Media and staff seconded to, or working for, contractors and vendors. For the purposes of this policy all these individuals are referred to as 'user' or 'users'.

The policy covers all activity on social media sites (both external- and internal- facing).
Users must comply with this policy when blogging in a professional capacity, or when adding comments to non-council social media sites or forums where they are giving the official corporate response, or when the content posted could be linked to their position within the council or to the council as a whole.

This policy shall not apply to schools and users that are not included in the paragraph above. Such users will need to comply with their own policies on social media use – but may themselves decide to adopt similar or identical policies outlined below.
This policy provides a structured approach to using social media and will ensure that it is effective, lawful and does not compromise Council information or 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 council or its business, nor be damaging to the Council's reputation and credibility or otherwise violate any Council policies.

2 Responsibilities

2.1 Who is responsible for this policy?

The Communications and Marketing team is the designated council owner of the Social Media Policy, Channel Strategy and associated appendices and is responsible for the maintenance and review of the policy. Queries about social media, this policy, strategy, or associated appendices should be directed to the Communications team.

2.2 Managers

Managers across SCC are responsible for ensuring that they are aware of any corporate social media activity occurring within their team or service area. They are required to understand this policy, and check that any social media activity happening is adhering to this guidance and in line with the corporate strategy. Managers should undertake regular assessments of the social media channels being used within their service area and those users charged with administering them to ensure continued compliance and to support users in accessing any necessary training or other corporate support. Managers wanting to create a new social media channel should refer to section 2.5 of this policy.

2.3 Social media users/administrators

Those charged with administrating social media tools must have read and understood this policy and have spoken to their managers about any social media tool they are charged with administering and have gained authorisation from their manager before administering any tool. All corporate social media must be undertaken in full compliance with this policy and the wider strategy and associated appendices.

2.4 Councillors

As a Councillor, if you use social media to help you to carry out your political work (rather than in your private capacity), your obligation to meet certain standards of conduct still applies. You can still be involved in robust political debate and state your opinions strongly – the policy does not exist to prevent you or fellow Councillors from expressing political views. It does, however, prohibit illegal behaviour, treating others with disrespect, bullying, and bringing one's office or authority into disrepute. See appendix 8.3 for more info about social media and councillors.

2.5 Requesting new social media accounts

Due to the risks associated with social media it is important that the council understands where all social media activity is happening. To achieve this, it is necessary to control the setting up and running of all social media accounts across the council. Therefore, **no-one** is authorised to set up any corporate social media account without first speaking to and gaining permission from the owner of this policy or another authorised member of the Communications Team. The team will work with the requestor to understand the business case, discuss the resource implications, understand how the channel will support the corporate strategy for social media and ensure that the chosen tool is appropriate.

2.6 Social media in partnerships

Often services are provided in partnership with other organisations and this can sometimes cause conflicts surrounding things like branding, names, colours or content. For social media the key is not the content but the administrator. If the account is administrated by a user as defined by section 1.3 of this policy, then this policy applies. If the account is administered by a partnership directly, or by anyone not outlined as a user, then this policy does not apply. Any new social media account where administration will be undertaken by a user must be approved in the same way as described in section 2.5 of this policy.

2.7 Training and support

SCC is committed to making sure that all users have the necessary and desired skills and training to enable them to use social media a safe and beneficial way. All staff should receive some training on social media before attempting to use any of social media tools available. Training is provided via Learning and Development – see mySCC for more information. Please remember to speak to your manager before booking any training course to ensure they understand what you are being trained on and for what social media account. Training can also be supplied by experienced colleagues or teammates, this peer-to-peer training can be very beneficial as it not only passes on knowledge of the platforms but helps maintain consistency relating to tone of voice used on the channel. If this training is not available, or the user still feels unsure about their role, further support training from the Communications Team can be provided.

2.8 Breaches of policy

This policy exists to protect the council and get the best outcomes from any corporate use of social media. Staff found to be in breach of this policy may be disciplined in accordance with the SCC Conduct and Capability Policy. In certain circumstances, breach of this policy may be considered gross misconduct resulting in dismissal.

Councillors found to be in breach of this policy may be deemed to be a breach of the Members' Code of Conduct leading to action by the Standards Committee.

Breach of Information Security - Users must report all suspected breaches of information security to the Information Management Team using the Information Security Incident report form on mySCC.

Data protection & Confidentiality – users must appreciate the open and publicly visible nature of any social media channel and must ensure that no personal, confidential, or sensitive data is disclosed without the explicit consent of individual / data owner.

2.9   Using Social Media for monitoring or surveillance

When carried out <u>in the course of a criminal investigation or operation</u>, any monitoring or surveillance of social networking or internet sites - or the establishment of a relationship on such sites in the guise of a member of the public - is likely to require magistrate's approval under the Regulation of Investigatory Powers Act 2000 (RIPA). The Council's lead RIPA officers are the Senior Authorising Officer (SAO), Mr Graham Crisp, Head of Trading Standards, graham.crisp@suffolk.gov.uk and the Senior Responsible Officer, Mr Nigel Inniss, Head of Legal Services. Please contact one of them if such activities are being considered.

3   Behaviours

3.1   What is meant by acceptable behaviours?

Social media behaviour is being developed by its users all the time. Depending upon the tool being used, it can force the use of abbreviations, demand posting techniques like including hashtags and encourages the sharing of other users work and content.

Therefore, acceptable behaviour is about more than just following this policy and being courteous to customers. It is about using tools in a way which enhances your message, builds your services reputation in your chosen channel and gets your message across.   You should follow adopted etiquette techniques for your chosen tools. As tool etiquette changes frequently – specific tool guidance should be searched for online first.

3.2   Tone of voice

It is important to remember that social media is a conversation between the council and one or more members of the public. The tone of voice used should be friendly, conversational and engaging.   As officers we must always be honest, helpful and keep true to our word. We should never judge, assume or guess – get the right answer first time, every time.

3.3   Adding value to conversations

It's not enough to just use any particular social media tool – the council must try at every opportunity to add value to people's conversations. By adding value, we believe that we can help people find the information they need quicker, empower residents to help themselves, build trust between communities and SCC and help reinforce that digital communication and engagement is the best way to interact with the council to make financial savings.

Adding value is easy – here are some simple tips.

- Know your boundaries as an Officer of the county council.   Are you the best person to answer the question? Do you know the answer, or are you assuming or guessing? If you aren't the best person find out who can. Pass the customer to the correct team, or if appropriate try and source the correct answer.
- Make sure you always try to answer a direct question. Never be afraid to say "I don't know, let me try and find out" – it is really important that you do actually try to find out the answer. No dead end conversations.
- Remember social media is a conversation, not just a platform to advertise services from. Officers need to listen as well as speak.
- Personalise the messages – the council is full of people not faceless logos and buildings. By adding your first name to tweets helps to build a feeling of a personal conversation which is exactly what social media really is.
- People are entitled to their feelings, beliefs and opinions. We may not always agree with them but officers should not look to engage in debate for or against them. Those sorts of conversations are best left to politicians and councillors.

- If things have gone wrong, or someone has a genuine grievance then apologise for it. Saying sorry doesn't mean you accept the cause to be unjustified – it just means you are showing empathy with the customer. You can then potentially examine ways of moving the situation forward if possible.
- Be clear upon expectations and limitations. If it is going to take a few hours or a few days to get the answer to a question, be honest and say so. Keep the customer informed throughout the time period. Users of social media expect an answer within hours, not days. If this isn't possible we should tell them so, and explain why.
- Keep your promises!

In reality adding value just means being a good listener and always trying to be helpful, honest and having a positive impact upon the conversations we get involved with.

3.4   Protecting people's personal data and information

When dealing with the public we must remember that social media is a public communication tool, not a secure or encrypted email. We must ensure that we do not request or publish any personal information about customers, their children or any other vulnerable dependant or person via social media. Such information would include a full name on sites where posting is anonymous or undertaken under an assumed profile name, full postal address, email, telephone number – or any other identity related material. We must also never request or accept bank details, credit card or debit card details via social media as the medium is not secure. In circumstances where it is desirable to take a conversation off social media, you should ask them to private message you with as little information as required to make secure contact outside of social media – this is normally just an email address.

3.5   Social marketing projects and communications

If you are considering a long term or major social media campaign – or other digital marketing exercise you should contact the Communications Team before starting. This will help you to gain advice on audience, key messages and see how your campaign may interact with other large corporate projects.

You can contact the Corporate Communications Team via email: communications.team@suffolk.gov.uk

3.6   Councillors

Acceptable behaviours of Councillors are outlined in the Councillor Code of Conduct. See appendix 8.3 for more information.

3.7   Personal accounts, accessing personal social media at work, professional accounts

The council recognises that social media for many of its staff members is now a normal part of their everyday lives. It understands that for many, as with our customers, social media is the way they connect with their families, receive their news and find out information. Therefore, the council will not seek to ban the personal use of social media during working hours but does advise staff that any such use should be minimal, proportionate and confined to lunchtimes and break periods whenever possible. Staff who use social media are encouraged to follow the council's social

media accounts – retweeting content and spreading council news, events and promotions. This is especially important during emergency situations and periods of increased public safety concern.

Whilst staff can make reference to their profession (i.e. carer or Government officer) they should avoid direct reference to their job title in such a way as to appear to be speaking in that capacity. Personal accounts are for personal postings – not for making statements on behalf of the council. The council does encourage the sharing of council generated news or information alerts. Council officers should refrain from making comments directly about SCC or its services and decisions.

When using social media sites that clearly state your occupation with SCC be mindful when displaying information that this does not cause offence or affect the reputation of the council. When using such sites to interact with work colleagues be mindful that content does not cause offence.

All staff should adhere to the Code of Contact when using social media in a professional or personal capacity.

In relation to their employment at SCC employees must be aware that disclosing the personal data of another individual, whether it be another staff member, customer or client, is a breach of the SCC Data Protection Policy as well as data protection laws.

Employees should be aware that any reports of inappropriate activity, linking them to the council, will be investigated.

With the rise in identity theft, blackmail and fraud, employees may wish to consider the amount of personal information that they display on their personal profile, as well as how often they review the privacy settings on all their social media accounts.

Some officers have decided to open a social media account in their professional capacity. The council recognises and accepts that this can be a useful tool for some services and departments, however, due to the necessity to ensure that the posts remain in step with wider council messaging all such accounts must be approved by the Head of Communications before going live. Any account set up must have a corporate look and feel, be named in terms of the role not the person, include the Suffolk County Council brand, be clear that it is a professional account in the description and all content must be professional and keeping in line with the role being talked about. The account should also link to the relevant pages on the council's website which talk more about the service or services.

The council can request the immediate deletion or censor of any social media account at any time.

3.8   Social media outside of working hours

Staff are **not** expected or required to monitor corporate social media accounts outside of working hours unless their contract of employment specifically states otherwise, and even then appropriate time off in lieu will be permitted.

There are occasions during emergency periods or periods of public safety concern where staff could be required to monitor and use social media corporately outside of working hours. The council expects such occasions to be rare and volunteers would be used in the first instance wherever possible, with appropriate time provided in lieu.

The county council supports staff to have a healthy work/life balance – and as such does not encourage social media users to access corporate accounts via personal devices or from home outside of working hours. All social media accounts should clearly state in the bio or the description the times/days which they will be monitored. This will ensure that the public have a clear understanding that we are not a 24/7 service and manage their expectation of receiving a response.

3.9   Dealing with online harassment and bullying (E-Safety)

Suffolk County Council is committed to creating a work environment where all employees are treated with dignity and respect in the workplace. It operates a zero-tolerance policy with regards to discrimination, harassment, and bullying. Separate polices exist to cover this.

Social media provides a platform for Cyber bullying, this is bullying, harassment and victimisation conducted through social media such as blogs or social networking sites.
If a member of staff feels they are being subjected to bullying, harassment or discrimination from anyone, they should speak to their manager or Human Resources immediately. The Communications Team should also be informed to alert other channels of the potential for abuse from that individual/s. Whilst the council would not wish to block anyone from contacting us using social media, persistent offenders or abusive customers can and should be blocked from all channels to protect staff from further abuse.

All Suffolk County Council employees are responsible for helping to ensure that individuals do not suffer any form of harassment and bullying, and that they are encouraged and supported in any legitimate complaint. Complaints that amount to an allegation of misconduct on the part of another employee will be investigated and dealt with under the disciplinary procedure.

Further information is available in the council's Bullying and Harassment policy which can be found on mySCC under the Ask HR tab.

For more information about E-Safety, protecting yourself and our customers online – please visit the pages on our website here: [http://www.suffolk.gov.uk/community-and-safety/staying-safe-online/. Additional information on how to protect yourself online, including social media security and tips on handling bullying visit Ask HR.](http://www.suffolk.gov.uk/community-and-safety/staying-safe-online/)

4   Protecting our reputation

4.1   Why reputation matters

Suffolk County Council is the leading authority for the people of Suffolk. It is therefore important that we build and maintain a positive reputation so that people trust us, take our advice and feel able to come to us with their problems and issues. If we create a bad reputation or damage our existing reputation it can take many years to repair or rebuild. Social media doesn't make it easier to damage a reputation compared to print or other traditional communication channels – it does however make the effect of that damage larger and easier for people to see and share.

4.2   How to protect our reputation

The easiest way to protect our reputation is to think before you post or reply. Follow a very simple posting/reply regime such as this. **If you are in ANY doubt get advice before posting**

Posting:

- Before posting consider the content of your post, is it political, is it controversial – will it require a sign off from a manager or councillor.
- Is this suitable for social media?
- Is there anything else happening on social media at the same time which might conflict with your message, or which your message might effect?
- Think about the sorts of questions your post will create – can we answer them, do you need to prepare some answers in advance?
- Are you using the right social media tool?
- Could someone else in the organisation be about to post something similar? We must look joined up.

Replying:

- Before you post anything read the original message again several times to ensure you have fully understood what is being asked.
- Are you the best person to respond? Or should you just respond to confirm receipt and advise escalation?
- Can you add value with a response? - is this just an opinion which the council should respect and remain silent about – or is this something which you can help with by offering advice or direction – People are entitled to their opinions – officers should not seek to debate their opinion with them.
- Has someone else in the organisation already responded previously, do you need to speak with them before replying? We must look joined up.

4.3   What to do when things go wrong - (Crisis Management)

It is important that we recognise that sometimes, regardless of a particular policy being followed, things will go wrong, and mistakes will be made. When this happens there can be an acute feeling to react in a certain way – deleting posts, shutting accounts or just hoping that the issue will vanish. This is perfectly natural, but is not necessarily helpful to resolving the issue.

All situations are different and a single policy prescribed approach is not possible – however, here is a process to help demonstrate how the council will deal with situations declared as a crisis, and those situations where we are dealing with negativity around a decision or service.

Crisis Management

It is important to know when your service or account may be involved in a crisis, however, it is also important to remember that not every "bad day" is a crisis either. It is very difficult to write a single process to deal with every "crisis" as each are unique and may require a different approach.

Generally, the best way to identify if your social media account is involved in a crisis is to consider the following points

- The subject is the only thing people are talking about negatively
- The subject is highly emotive or represents a high reputational risk
- The subject is legal in nature – or has negative legal connotations
- The press has picked up on it and are reporting it negatively

If after consideration you think your account is in crisis – post a "listening response" and then STOP posting/responding immediately, collect as much information from the account and the contributors as you can (who is talking, how wide is their following, how frequently are they posting, are others joining in, hashtags being used etc.), alert your manager and contact the Communications Team.

The Listening Phase

When a crisis hits, one of the most important things to do is to start to listen more than you speak - every post you make will come under greater scrutiny, so it is important that each one is thought out, measured, contains the correct key messages and is authorised by the right stakeholders. Ensure that all the information about a situation is captured and processed before deciding upon next steps.

One thing which will generate more negativity for the channel is silence – people will often attribute this to either the council being afraid to respond or worse still them being ignored. The best way to avoid this is to issue a "listening response" – which can be something as simple as "Thank you for bringing this to our attention, we are investigating and will respond as soon as we are able – we are listening". That will buy you the time to assess the situation, let the stakeholders know and form the Crisis Management Group and to get further guidance.

Crisis Management Group

It is important that if your channel is embroiled in a crisis that you are able to alert and gather appropriate stakeholders to help make the decisions of how to proceed. The group should be made up of a member of the Communications Team, your manager, maybe the service lead in some cases the cabinet member or local councillor. The group should consider what's happened, what's been said already, the accuracy of the statements being made and look to formulate key messages to use through the crisis period. It is also helpful to appoint one person as the approver for all messages to be posted on the social media account during the crisis period. That enables better control of the message. Crises does not end at 5pm – the group should decide whether to extend working beyond normal working hours.

Response phase

The Crisis Management Group will need to form an agreed response as soon as possible. Remember the listening response is only a holding statement.
Things to consider when formulating responses:

- What format will the response take, a tweet, a post, a statement, a press release – all of the above?
- Is this a political response or a service response – who is speaking?
- Does it answer the questions asked?
- Is information in the public domain?
- Does it show empathy towards the situation?
- It is appropriately worded – plain English, avoiding the council jargon
- Does it need to sound empathetic or authoritative?
- Have we updated websites with the correct information?
- Have all stakeholders been briefed?
- Don't try to spin – transparency is always the best policy
- If we are sorry – have we said we are sorry?

When answering, make sure to plan ahead – what are the potential follow up questions, can we include them in the original messaging, can we prepare responses or provide published FAQs.

Make sure that all political stakeholders are briefed in case of being door stepped by journalists.

Once the response is made – return to the listening phase and listen again to what is being said. Feed any new information into the Crisis Management Group for consideration and response.

It is also necessary to review membership of the Crisis Management Group throughout the period of activity, the right stakeholders at day one may not be the right stakeholders by day two.
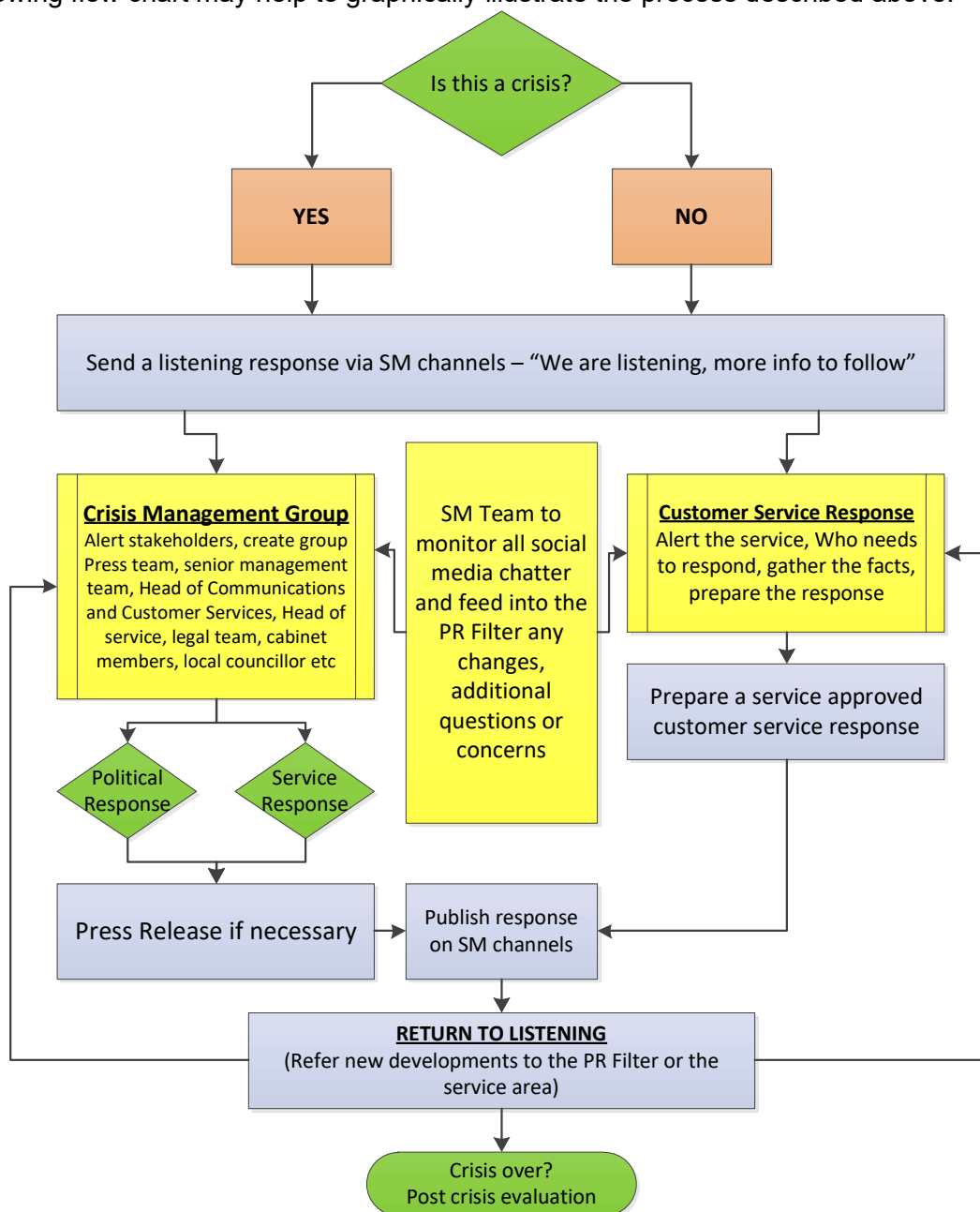
Continue with the approach until the channel returns to pre-crisis topics and the level of attention drops away. Normal service has resumed.

Post crisis

As important as actually dealing with a crisis is the evaluation afterwards. What happened, why the crisis occurred, what can be done to try and make sure this doesn't happen again? You should also do an analysis of the channel, how has the account been left in terms of followers and reputation, is it worth continuing, consider rebranding or starting again?

Get help with this from the Communications team – metrics and statistics are available for some social media tools.

The following flow chart may help to graphically illustrate the process described above.

```
                    ╔═══════════════════╗
                    ║  Is this a crisis? ║
                    ╚═══════════════════╝
              ┌──────────┘        └──────────┐
        ┌──────────┐                   ┌──────────┐
        │   YES    │                   │    NO    │
        └──────────┘                   └──────────┘
              │                              │
┌──────────────────────────────────────────────────────────────┐
│ Send a listening response via SM channels – "We are listening,│
│                    more info to follow"                        │
└──────────────────────────────────────────────────────────────┘
```

Crisis Management Group
Alert stakeholders, create group Press team, senior management team, Head of Communications and Customer Services, Head of service, legal team, cabinet members, local councillor etc

SM Team to monitor all social media chatter and feed into the PR Filter any changes, additional questions or concerns

Customer Service Response
Alert the service, Who needs to respond, gather the facts, prepare the response

Political Response

Service Response

Prepare a service approved customer service response

Press Release if necessary

Publish response on SM channels

RETURN TO LISTENING
(Refer new developments to the PR Filter or the service area)

Crisis over?
Post crisis evaluation

5 Social Media Single Access Platform

5.1 What is a Social Media Single Access Platform?

The Social Media Single Access Platform (SMSAP) is an administration and engagement tool used to bring together the various council run social media accounts into one software platform. The platform is a third party developed software which is internet browser based, based in the cloud (meaning not on the SCC network) and is administered by the Customer and Online Services team on behalf of the entire council.

5.2 Benefits of using a Social Media Single Access Platform

The SMSAP provides the following benefits to the council

- Secure social media accounts by having trained users logging into the platform rather than the accounts
- Pulls together social media engagement into one place allowing the council to monitor and report upon activity as a whole.
- Allows for better communications between social media users regardless of service or account – greater flexibility of staff and better support for moderation and editing before publishing
- It enables the council to see clearly who is involved in social media activity and in what capacity
- Reduces the risk of leavers continuing to have access to accounts when they no longer work for the organisation. Or vice versa, account details being lost when people leave the organisation as they were the only ones who knew the login details.

The SMSAP provides the following benefits to the social media account administrator

- Allows you to create a team of users around your account/service
- Helps schedule your content over the course of the year with a publishing calendar
- Allows moderation of content and setting up of approval processes unique to any particular team or account.
- Allows tagging of social media posts using self-generated tags which can be reported upon to see activity around a particular topic.
- Gives the ability to assign social media posts outside of the platform to experts and others in the council for answer and response.
- Prioritise messages from customers which need urgent answers
- Channel reports and team activity reports

5.3 Current Social Media Single Access platform provision

The current SMSAP provider for Suffolk County Council is Orlo (**www.orlo.tech**)
They were appointed in April 2021 for a 2-year contract.

5.4 How to get my social media account added to the platform and gain training.

You should speak to the Communications Team who will discuss with you the details of your account, the number of administrators and confirm whether the account is able to be added or not.

Training on the platform is provided by the supplier but due to the simplicity of the platform the training takes approximately one hour to complete.

5.5 Managing social media accounts which are not managed via the single access platform

Not every type of social media can be managed via the SMSAP – this is due to the technical way some social media accounts work leaving them incompatible with the SMSAP technology. Current supported networks are:

- Facebook
-
- Twitter
-
- Instagram
-
- LinkedIn

If your account cannot be monitored via the SMSAP you should still follow this policy and the corporate channel strategy for social media. In addition to following the standards laid out in this policy you should also ensure that your social media account is registered with the Communications Team. This registration will include the login details for the account in question so that should anything happen the council can still gain access to the account. You should also ensure that should a member of the team with access to the account leaves, that all passwords are changed and that the centrally registered details are updated immediately.

You should make sure that access to your social media account is as secure as possible, and that access is not shared with anyone unnecessarily. Keep a list of those people who have access, and change the password regularly, especially when anyone with access leaves the organisation or changes job.

6   Legal and supporting policies

6.1   Authorisation, Approval dates and review dates

This policy is written by the Senior Communications Officer (Digital and Social Media Specialist) and is authorised by the Head of Communications and Media on behalf of the Corporate Leadership Team.

Version control details are at the front of this policy

This policy will be reviewed by the Senior Communications Officer (Digital and Social Media Specialist) annually from the date of last approval.

6.2   Audit Requirements

This policy, along with social media in general will be subject to corporate audit by Scrutiny and Monitoring in accordance with corporate auditing policies.

6.3   Equality Impact Assessment

In accordance with equality polices this policy has been subject to Equality Impact Screening and following a decision from the Policy Clearing House did not require a full Equality Impact Assessment. (Decision taken 25 August 2015)

6.4   Legal Requirements

The following legal documents have a bearing, or impinge on the rationale of this policy:

- Data Protection Act 1998
- Freedom of Information Act 2000
- Human Rights Act 1998
- Communications Act 2003
- Local Government and Housing Act 1989
- Local Democracy, Economic Development and Construction Act 2009

6.5   Associated reading and policies

- The Acceptable Use of IT policy
- The E-Safer Suffolk E-Safety Strategy
- Councillor code of conduct
- Code of Conduct Policy
- Politically restricted post guidance

6.6 Alternate policy formats

If you would like this policy in a different format please contact:

Matt Woor
Senior Communications Officer (Digital and Social Media Specialist)
Email: matt.woor@suffolk.gov.uk
Suffolk County Council
Endeavour House
Russell Road
Ipswich
IP1 2BX

7 Glossary

Hootsuite provide social media platform technology, they also provide a great social media glossary which is freely available here.
https://blog.hootsuite.com/social-media-definitions/

8 Appendix

8.1 Freedom of Information Requests

The Freedom of Information Act gives everyone the right to request written or recorded information held by Suffolk County Council.

The Environmental Information Regulations Act 2004 (EIR) allows access to information about the environment e.g. water and air quality, and details of animal and plant life in Suffolk.

Data protection provides access to information held by Suffolk County Council that constitutes personal information covered by the Data Protection Act.

Requests for information can be made through any social media site that the county council uses or has responsibility for not just the corporate SCC Facebook or Twitter site.
Requests themselves may be made publicly on the sites or via private/direct messages. The public don't always make it clear when they request information whether they are wanting to make a Freedom of Information request or not. Sometimes they pose questions to make a point rather than actually make a request. If you are unsure you can always ask the customer whether they want their questions to be considered under the FOI act and then handle it accordingly.

Freedom of information requests must be responded to within 20 working days. If such a request is received (or you are unsure if a request falls under FOI), please forward to the Information Governance team at foi@suffolk.gov.uk as quickly as possible.

Remember to update the customer either publicly or by replying to their private/direct message thanking them for the making the request and informing them of the next steps. Where an email has not already been provided a suggested response is.
"Thank you for your request. Our Freedom of Information team will be in contact with you shortly. In the meantime, you may wish to provide the team with a direct email address to send the response to, if you would like to do this please contact foi@suffolk.gov.uk or reply to this message with an email address we can use."

Twitter style response

"Thanks for the request. Please DM us your email and we will pass that on to the FOI team who will be in contact shortly."
If the requestor does not wish to provide an email or suggests they want us to use the social network to answer the question, the request is still valid and must still be handled by the FOI team in the same way. Make sure that the question is emailed to the FOI team foi@suffolk.gov.uk and thank the customer for the question. Also email the Communications Team to let them know too.

If in ANY doubt, contact the FOI team immediately as there are statutory time limits in place.

8.2   Suffolk Fire and Rescue Service

1.   Introduction

This document states the ways Suffolk Fire and Rescue Service (SFRS) approach social media that may be different to the Suffolk County Council Social Media Policy.

The Suffolk County Council Social Media Policy is the overarching policy that must be adhered to, apart from the difference stated below.

2.   Responsibilities

2.1   Social media users/administrators
All administrators or users should have read the SCC policy including this appendix and received the necessary social media training from Suffolk County Council (SCC).

2.2   Emergency planning situations

During an emergency scenario the social media response will be dictated by the department, or body in charge of the incident, our social media feeds will be used to give out information to the public, either by re-tweeting or sharing the required information.

2.3   Requesting new social media accounts

Any requests for new social media accounts should be discussed with the Business Support Manager or AC Support Services; they will then approach the Suffolk County Council Communications Team who will consider the request. A list of account holders will be held by SFRS Business Support Manager.

2.4   Individual station accounts

A Suffolk Fire and Rescue Service social media administrator should also have administration rights to any individual account. The administrator will help to insure administration rights are taken away when people leave and to insure accounts are managed within the protocols set out by this appendix and the Suffolk County Council Social Media Policy. Please see paragraph 5.1 for more information.

2.5   Standards expected

Specific incident details are not to be discussed over open social media forums, this includes:

- Details of firefighter numbers in each appliance.
- Crews off the run.
- Casualty details.
- Fatality details.
- Any official sensitive information.
- Incident details linked specifically to an individual or exact location.
- ILO information.
- Sensitive operational information.

As well as the above, attacks or posts perceived as bullying using social media on individuals and departments within SFRS and SCC will not be tolerated.

Any information requested that is not appropriate to respond to using social media, the person asking will be asked to fill out a Freedom of Information Request.

3.   Standards Expected

This policy exists to protect SFRS and to achieve the best outcomes from any corporate use of social media. Staff found to be in breach of this policy may be subject to disciplinary proceedings in accordance with the Suffolk County Council Disciplinary procedure policy.

3.1   Breach of Information

Security Users must report all suspected breaches of information security to the Suffolk County Council Information Management Team using the Information Security Incident report form on mySCC.

3.2   Data protection and confidentiality
Users must appreciate the open and publicly visible nature of any social media channel and must ensure that no personal, confidential or sensitive data is disclosed without the explicit consent of individual/data owner.

All administration users should undertake basic safeguarding training. To be arranged via the Prevention Manager.

4   **Photographs and Video from Incidents**

4.2   Photography at incidents

Photographs and videos from scenes are acceptable but should only be taken after permission is given from the officer in charge. Photographs and video should not be uploaded to social media sites whilst still at the incident, unless the footage would benefit the public, for example during a major incident it may be beneficial to give information out to the public sooner rather than later. If this is the case then the officer in charge of the incident should post directly to the necessary site, or contact a social media administrator to post on their behalf.

Any footage taken should be sent to a social media administrator via WhatsApp, e-mail or as a direct message on a social media platform as soon as the photographer is able. Upon receipt the content/footage should be checked, looking out for the following:

- Any personal items.
- Signs of death.
- Distinguishing features of a property including house number.
- Number plates.
- Inappropriate PPE.
- Casualty faces.
- Children and young adults under the age of 18.

If any of this is found on the photograph or video, then the feature should either be deleted using manipulation programs or the photograph or video must not be uploaded to any social media site. If the administrator is in any doubt on whether the content/footage is suitable for use on social media, they should check with a Station Commander or above.

Once the photograph or video has been cleared for use then it should be posted to the necessary social media sites with a description of the incident, the action the Fire Service took and links to any safety information available, either on the SCC website or a suitable partner website. Please see picture below as an example:

4.3 Photography and video while at work

Permission must be obtained prior to photographing or filming.
Parental permission must be obtained to photograph or film any child under the age of 18, this should be in writing and a form can be found on MySCC. Children under the age of 18 can be included in photographs or video without parental permission if the child is unrecognisable.

5 **Behaviours**

5.1 Adding value to conversations

Know your boundaries when posting on social media sites. Are you the best person to answer the question? Do you know the answer or are you guessing? If you do not know the answer, ask somebody who may know. For example, if the question is about an incident, ask the officer in charge of that incident for more information.

We currently do not use names on messages and tweets, but that does not mean you cannot end the conversation in a friendly way. Try and end with a safety message and then add Suffolk Fire and Rescue Service, for example:

Hi Paul,
Please can you DM (direct mail) us with some more information?
Thank you
Stay Safe
Suffolk Fire and Rescue Service

5.2   People are entitled to their feelings, beliefs and opinions

We may not agree with them but you should not look to engage in debate, or delete posts that ague against the Services policies. However, if the information being debated is wrong or contains misinformation then a reply can be written as long as the information contained is 100% accurate and will not encourage more detailed debates with individuals.

5.3   When should a post be deleted?

A post should only be deleted if it falls into any of the criteria below:

- Broken the law, this could be because of abuse, harassment or abusive behaviour.
- Profanity (Swearing).
- Naming of the general public and linking them to an incident.
- Hate crime, for example inappropriate language when describing ethnic groups. If the post falls into this category, then it will need reporting to Suffolk Hate Crime Services

In each case the reason for the post deletion will need explaining to the poster on the affected thread. If the post contains profanity or is able to re-post without the offensive section, then it should be explained to the poster that this is an option.

5.4   Social Marketing Projects and Communications

If you are considering a long term or major social media campaign, please contact the necessary person within Fire Business Support who can support you in finding out what is required before passing onto the Communications Team. Please refer back to the Suffolk County Council Social Media Policy for more information.

5.5   Personal and professional accounts

Without the necessary permission from the Chief Fire Officer and the Head of Communications and Media at Suffolk County Council social media accounts are not official and therefore should not be described as such. If your current social media profile is dedicated to your current role, administration rights will need to be given to a SFRS social media administrator.

Whilst staff can make reference to their profession, they should avoid direct reference to their job title in such a way as to appear to be speaking in that capacity. Personal accounts are not for making statements on behalf of Suffolk Fire and Rescue Service.

SFRS wishes to share information as regular and often as possible via social media, this will be posted by senior managers in conjunction with SCC Communications Team, as well as the person responsible for the everyday running of SFRS social media profiles.

6   **Protecting Our Reputation**

6.1   Why reputation matters
It is important that Suffolk Fire and Rescue Service build and maintain a positive reputation so that people trust us, take our advice and feel able to come to us with their problems and issues relevant to the Service. Damaged reputations can take many years to repair or rebuild. Social media doesn't make it easier to damage a reputation compared to print or other traditional communication channels – it does however make the effect of that damage larger and easier for people to see and share. For more information, please refer back to the Suffolk County Council Social Media Policy.

6.2   Breaches of this policy
Any breaches of policy may be dealt with in accordance with the Suffolk County Council Conduct and Capability Policy.

6.3   Complaints about social media posts
Any complaint about social media posts should be dealt with quickly and effectively. Depending on the severity of the complaint the post in question should be removed, and communication given back to the origin of the complaint about any investigation, and / or reasoning for the uploading of that post.

If the original post does not need removing then a reply should be given on the post in question with all reasoning why that particular post is fine to use, if the conversation is longer than an initial reply and thanks, take the conversation offline by asking the other party to DM us.

All complaints will be dealt with by the person/department responsible for the everyday running of SFRS social media profiles in the first instance, who will escalate if required. To highlight incorrect posts e-mail fire.businesssupport@suffolk.gov.uk or DM the social media feed the post appears on.

8.3

SOCIAL MEDIA PROTOCOL FOR MEMBERS

Purpose of this protocol

The Council welcomes Members' use of social media and would like to support this by giving guidance so that Members have greater clarity as to what is and is not acceptable usage of social media. This protocol is intended to provide such guidance and complements the general rules under the Suffolk Local Code of Conduct for Members.

What are social media?

Social media is the term to describe websites and online tools which allow people to interact. This could, for example, be blogs, and postings on a wide range of social media platforms including (but not limited to) Facebook, Twitter, Linked in, snap chat, integral etc.

On many social media sites users share information, give opinions and may create interest groups or pages leading to longer exchanges. Ultimately people use these sites and tools to build online communities and networks which encourage participation and engagement.

Social Media and Members

It is not a requirement for Members to have a Facebook or Twitter account or to use other forms of social media to fulfil their job as a Member. However, if you are using or planning to use social media in connection with your work as a Member or are already using such media in your private capacity, these guidelines will be relevant. Remember that, whenever you act or appear to act in your official capacity, you must comply with the Code of Conduct.

Social Media can be used;

- To support members in performing their community leadership role
- To keep in touch with or obtain local views and opinions
- For political campaigning
- For campaigning on local issues

Types of Social Media:

- Blogging and micro blogging – online journals – Twitter is an example of micro blogging, where entries are limited to 280 characters
- Online Forums – people with similar interests sharing information and opinions – AccyWeb is an example
- Social networking sites – these facilitate connections between who already know each other, often in a social context, but are increasingly used by businesses to promote their products or services - Facebook is an example
- Video and photo publishing – sharing videos and photographs worldwide – Instagram is an example

Things to bear in mind

- Any communication is capable of being misinterpreted. While the use of social media should not be more susceptible to this problem than any other form of communication, something about the immediacy of social media seems to magnify the problem.

- By the nature of such media, misinterpretation, or misrepresentation, particularly with regard to something that is perceived as being more controversial than it was expected to be, is likely to lead to rapid and wide broadcasting of that apparently "controversial" item.

- There are no special, additional legal or ethical burdens relating to the use of social media. The same rules apply here that govern the rest of your behaviour as a Member – you just need to think about them in this new context – their immediacy and ease of dissemination.

- Although the best use of social media is conversational in tone, publishing to the web is still publishing. What you've said on the web is recorded and it is permanent. Most pitfalls will be avoided if your online content is accurate, informative and thought through. Think of it as speaking in public. Think before you commit each word.

- This doesn't mean that members cannot, in the appropriate context, communicate politically. This is expected of a member, but you should be careful not to say anything that you wouldn't be comfortable repeating or justifying, for example, at a public meeting.

Some legal issues:

- **Libel –** If you publish an untrue statement about a person which is damaging to their reputation, they may consider it as defamatory and consider legal action. The same thing may happen if, for example, someone else publishes something defamatory on your website; you know about it and don't take swift action to remove it. A successful legal claim could result in the award of damages against you.

- **Copyright –** Placing images or text on your site from a copyrighted source (for example extracts from publications or photos), without obtaining permission, is likely to breach copyright laws. Therefore, don't publish anything you are unsure about, or obtain prior permission. Again, a successful claim for breach of copyright would be likely to lead to an award of damages against you.

- **Data Protection –** Do not publish the personal data of individuals unless you have their express permission. Personal information in an email or personal exchange should not be presumed to imply any consent to pass it on to others. If you place personal information on a public forum you should expect it to be published by others.

- **Bias and Predetermination –** if you are involved in making planning, licensing or other quasi-judicial decisions, do not say anything through social media (or indeed anywhere) that suggests you have made your mind up on an issue that is due to be formally decided. While your likely view on a particular application may be well known, you need to be able to show that you attended the committee or hearing prepared to take on board and weigh all the evidence, and were genuinely persuadable to a different view, otherwise, the decision may be later challenged as invalid. If a person has suffered some sort of detriment as a result of such an invalid decision, they may have a claim against the Council for damages.

Social Media and the Suffolk Local Code of Conduct for Members generally:

- Aspects of the Suffolk Local Code of Conduct for Members will apply to your online activity in the same way as they do to any other communication you may use. The key to whether your online activity is subject to the Code is whether you are, or appear to be, acting in your capacity as a Member rather than as a private individual.

- It can be presumed by others that you are speaking as a Member. This can happen where you have a social media account where you comment both as a Member and as an individual. Although you may be clear in your mind that you are acting in a private capacity it may be less clear to others. This can also mean that your views can be taken as being those of your organisation or party (rather than you personally) when this may not be the case.

- The presumption can arise simply because you are commenting on Council business, because you are known to be a Member or make reference to this, use party political symbols or references in the text.

- One way of avoiding this, and avoiding some of the potential problems related to the Code of Conduct, may be to consider keeping your online accounts as a Member separate from those where you communicate in a personal capacity. Another is to spell it out in the text (e.g. "speaking entirely personally…"). This is a decision for each member and some members may find the convenience of having one account outweighs the advantages of separate accounts. The Council's Communications Team can help you with more specific advice if needed.

Relevant Elements of the Members' Code of Conduct:

- **You must treat others with respect** - do not use social media to make personal attacks or indulge in rude, disrespectful or offensive comments.

- **You must comply with equality laws** – do not publish anything that might be racist, sexist, ageist, homophobic or anti-faith.

- **You must not bully or harass anyone** – do not say anything, particularly if it is part of a series of similar comments about a person or on a theme that might be construed as bullying or intimidation.

- **You must not bring your office or the Council into disrepute** – you should not publish anything that could reasonably be perceived as reflecting badly upon or lowering the reputation of you or the Council.

- **You must not disclose confidential information** - you must not, in your use of social media, just as in any other circumstances, disclose information given to you in confidence by anyone, or information acquired by you which you believe, or ought reasonably to be aware, is of a confidential nature. Inadvertent leaks of the Council's confidential information are more likely to take place when a member is using social media, rather than, say, when they are carefully drafting a letter for publication in the local paper. This may be because of the more immediate, conversational, off-the-cuff nature of much social media communication. Members must be careful to apply exactly the same standards to their social media communications as they would to statements made in a more formal context.

Staying out of Trouble - Some Do's and Don'ts

Some Do's

• set appropriate privacy settings for your blog or networking site – especially if you have a private, non-political blog.

• keep an eye out for defamatory or obscene posts from others on your blog or page and remove them as soon as possible to avoid the perception that you condone such views. Be aware that the higher your profile as an elected member, the more likely it is you will be seen as acting in your official capacity when you blog or network.

• consider keeping your personal and elected member profile on social networking sites separate and maintain appropriate professional boundaries.

• ensure you use Council facilities appropriately; if you use a Council provided blog site or social networking area, any posts you make will be viewed as made in your official capacity.

• be aware that you will be seen as acting in your official capacity if you publish information that you could only have accessed by being an elected member.

• feel able to make political points, but be careful about being too specific or personal if referring to individuals. An attack on individuals may be seen as disrespectful, whereas general comments about another party or comments on policy are less likely to be viewed as disrespect.

• recognise the positive, don't just use it to criticise. Say thank you.

• Keep blogs, Facebook pages etc up to date and relevant.

Some Don'ts

• blog in haste, particularly in circumstances where your judgement might be impaired; for example, if you are tired or have consumed alcohol.

• post comments that you would not be prepared to make on paper or face to face.

• use Council facilities for personal or political blogs.

• request or accept a Council employee or contractor providing services to the Council as a "friend" on a social networking site where this suggests close personal association. For the avoidance of doubt, this does not apply to sites which are intended as a neutral, professional connections registry (such as LinkedIn).

• use social media in any way to attack, insult, abuse, defame or otherwise make negative, offensive or discriminatory comments about Council staff, service users, their family or friends, colleagues, other professionals, other organisations, or the Council.

- publish confidential information that you may have learned or had access to as part of your role as an elected Member. This includes personal information about service users, their families or friends or others e.g. contractors, Council staff as well as Council related information.

- represent your personal views, or those of any political party or interest group you belong to, as being those of the Council, on any social medium.

- browse, download, upload or distribute any material that could be considered inappropriate, offensive, defamatory, illegal or discriminatory.

- make conspicuous or excessive use of social media technology during the course of a Council or committee meeting so that you give the impression to the public of not being respectful of the proceedings and, more seriously, taking decisions that are not based on full engagement with the facts and arguments.

General

The Council wishes to encourage Members' use of new technology, including social media. This guidance is intended to help Members use social media in a way that avoids legal and reputational risk.

The Monitoring Officer and the Communications Team are happy to help Members by providing additional advice and guidance as appropriate. Training is also available to individual Members or Groups.