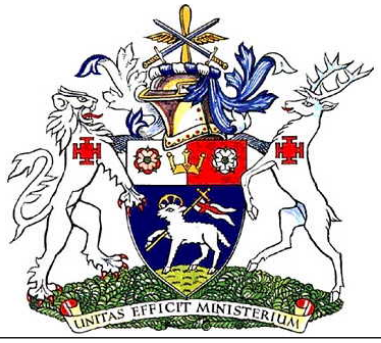	**General Functions Committee** **11 November 2015**
Title	**Communications with the Public by Text and Social Media for Members Policy**
Report of	Jenny Obee, Head of Information Management
Wards	All
Status	Public
Urgent	No
Key	No
Enclosures	Appendix A: Communications with the Public by Text and Social Media for Members Policy
Officer Contact Details	Victoria Blyth, victoria.blyth@barnet.gov.uk, 020 8359 2015

Summary

This report asks the Committee to comment on and approve the Communications with the Public by Text and Social Media for Members Policy which forms part of the Members' Information Management Policy.

Recommendations

1. **That the Committee comment on and approve the Communications with the Public by Text and Social Media for Members Policy which, subject to approval, forms part of the Members' Information Management Policy.**

1. WHY THIS REPORT IS NEEDED

1.1 With the rise of social media and text messages as common communication tools, especially with young people, the council has considered the Data Protection Act 1998, associated case law and regulatory guidance to produce

a policy for staff on using social media and text messaging to communicate with customers.

1.2 That policy explains how data protection standards and duties can be maintained with social media communications where personal data is being communicated and staff must comply with it.

1.3 Following the Committee's comments on that policy (12 October) the attached policy (Appendix A) has been designed to offer guidance to Members on how they may be affected by legislation in this area. Subject to the committee's approval, it is proposed to form part of the Members' Information Management Policy.

2. REASONS FOR RECOMMENDATIONS

2.1 The General Functions Committee requested that a policy be drafted to provide guidance to Members on their use of social media to communicate with the public and explain their responsibilities. It is suggested that this new policy be appended to the Members' Information Management Policy.

2.2 This policy on social media is intended to promote understanding of the responsibilities of a Member and corresponds to the different capacities within which they carry out their work (referenced in section 3 of the Members' Information Management Policy). The Members' Information Management Policy explains how these three distinct roles have different rights of access and accordingly, different obligations under information legislation.

3. ALTERNATIVE OPTIONS CONSIDERED AND NOT RECOMMENDED

3.1 Guidance for Members could be incorporated to an existing staff policy but it is suggested that its attachment to the Members' Information Management Policy would assist to maintain a clear delineation in its application to councillors.

4. POST DECISION IMPLEMENTATION

4.1 Subject to the committee's approval, the policy would be published on the council's website and communicated to Members.

5. IMPLICATIONS OF DECISION

5.1 **Corporate Priorities and Performance**
N/A

5.2 **Resources (Finance & Value for Money, Procurement, Staffing, IT, Property, Sustainability)**

5.2.1 None in the context of this report.

5.3 **Social Value**
N/A

5.4 **Legal and Constitutional References**

5.4.1 The Communications with the Public by Text and Social Media Policy is written to assist the council in meeting its obligations under the Data Protection Act 1998 (DPA) and in addition to legislation, it considers best practice from the regulatory body, the Information Commissioner's Office (ICO) and recent case law. This new policy specifically for Members will assist the council in meeting its data protection responsibilities, and assist Members in meeting their obligations under the DPA for which they are individually responsible.

5.4.2 The General Functions Committee's Terms of Reference are outlined in Section 15a of the Constitution, Appendix A to Responsibility for Functions, which states that the committee is responsible for all other Council functions that are not reserved to Full Council.

5.5 **Risk Management**

N/A

5.6 **Equalities and Diversity**

None

5.7 **Consultation and Engagement**

None

5.8 **Insight**

None

6. BACKGROUND PAPERS

6.1 Members' Information Management Policy

6.2 Communications with the Public by Text and Social Media Policy (Barnet Council employees)

6.3 General Functions Committee Minutes (Item 11 – Resolution) 12 October 2015

Appendix - Communicating with the Public by Text and Social Media for Members Policy

1. Introduction

Councillors acting in their capacity as a Member of the Council must follow this policy to ensure that the council is abiding by the Data Protection Act (DPA). It does not formally apply when they are acting in their capacity as a ward councillor or in their role representing a political party, as these are not the responsibility of LBB. The three roles of Members are set out in section 3 (The role of the elected Member) of the main policy. However, Members may find this guidance a useful reference in helping them meet their individual data protection responsibilities as Members in their ward councillor or political party member roles.

In our modern society people wish to communicate with their councillors in many different ways. Equally, some councillors may wish to communicate with their constituents in different ways. Whilst many still communicate by traditional letter, telephone or email, others wish to use more modern methods. These include (but are not limited to) the familiar and well established such as text message, and newer methods such as instant messaging services (eg BBM (Blackberry Messenger), IM (Instant Messenger), What's App etc) or twitter, Facebook, Skype etc. In this policy we refer to all of these methods as "social media". It is recognised that the number of social media applications and websites is likely to increase over time and this guidance applies to new social media sites as well as existing interfaces.

It is helpful to allow people to different platforms to communicate with their councillors about council business. These are likely to include using social media. When using social media to communicate with the public it is important that proper care is taken to ensure that personal data is handled properly.

It is also important to note that there is no pressure on Members to use social media methods that they do not feel comfortable using.

1.1. General points

The Data Protection Act (DPA) principles apply to social media communications containing personal data/ sensitive personal data in just the same way as any other communication method. Although social media may be a more informal tool the same standards of data protection need to be applied as to more traditional communication methods.

The same common sense rules apply to social media communications as they do to more traditional communications. The more informal nature of social media can occasionally lead people to respond too quickly, so we recommend taking a moment to consider whether the communication is fully formed and appropriate. If Members have any concerns regarding their proposed response to a member of the public via

text or social media, it is recommended that they seek guidance from the Information Management Team. This will help to ensure the council is meeting its legal obligations in relation to data protection, as well as supporting Members in their role. See section 13 above for how to contact the Information Management Team.

Not all social media communications are public (eg texts, private messaging) therefore, like email, communications with the public by social media by Members in their Council Member role should be on council issued/approved devices in order to maximise security of personal data. Councillors' personal devices should not be used to communicate with members of the public for *council business* matters or ward councillor matters. They can of course be used for political communications.

1.2. Permission

When a constituent first begins to deal with a councillor they will usually provide their preferred contact details. This will be the method the Member generally uses to contact them. If the Member wishes to contact them by a social media method not used previously, ensure you have their permission to use that social media method. Not all Members will wish to use social media to communicate with constituents and it is acceptable for the Member to advise the constituent that traditional communications will be used, even when the constituent requests to be contact via a social media channel. Although Members must ensure that they have the correct alternative contact details of the constituent.

Members should not assume because someone who usually emails you has also given you their mobile number, that they will want to receive text messages. If a Member wishes to text it would be advisable to first ask the constituent whether this is acceptable, ensuring you do not put undue pressure on them. If they agree make a note of the permission.

- For example, a member of an Area Planning Committee may be discussing a forthcoming planning application with an objector by text. The person may mention that they prefer What's App (for example) as it uses Wi-Fi and doesn't count towards their text allowances. If the Member is happy to use What's App then before communicating via this method the Member should check that the person wishes to communicate in this way and ensure they have the correct user name. They can then message through What's App.

1.3. Correct Contact Details

It is vital that Members ensure they have the correct contact details for the mobile phone or social media channel. Constituents' user names on social media channels are likely to be different to the person's name and so the details should be checked with the constituent before communicating via that channel. This is especially important with applications where user names may not be the same as a person's name, or where several people have similar user names.

If a Member has not used a particular communication method before it is advisable to send a test message to the member of public asking the recipient to contact the Member. When they contact you and verify their identity verbally you will know the number/user name is correct.

People often change their user names and mobile numbers frequently and after a period of non-use it is wise to check they are still current. If you have not contacted the person for a period of time and then need to after, say 6 months, you should check that the details are still valid as described above.

- For example you might say in a text, “Hello Jim Smith it’s Councillor Smart from Barnet Council, I need to contact you about the Planning Committee meeting next week, could you please call me on XXXXX thanks.”

1.4. Minimise Personal Data Sent

Social media messaging is not always as secure as other methods and mobile devices are targets for thieves. Members of the public are unlikely to have the same level of security on their devices as councillors have on council issued equipment. Texts and other instant messages on constituents’ mobile phones/devices may be read by others accidentally or deliberately. Therefore to reduce the risks of personal information going astray Members are advised to keep the amount of personal information in social media messages to the minimum required. This is especially important with sensitive personal information.

Where communications involving sensitive personal data need to be made with a member of the public these should generally be done by more secure means than social media. For example, email is as quick but more secure than text or other messaging services. Where contact does need to be made through social media, especially where this is the usual way of communicating, a message requesting contact should be made instead of sending sensitive personal information.

- For example instead of saying in a What’s App message “Hello Jane Bloggs, its Councillor Smart. I spoke to the Licensing Officer about your alcohol license hearing next week, and the objection received was because you have a conviction for selling alcohol to underage people”

  You could say “hello its Councillor Smart, I spoke to the council officer as you requested and I need to update you. Please give me a call on XXXX”

1.5. Twitter

Members should endeavour to be clear when using their public social media accounts, such as Twitter, whether they are posting in a personal or council/ward councillor capacity. Members may wish to set up accounts specifically for council business to separate their personal and professional messages.

Members can of course tweet political messages (in their Members' "political" role- see section 3 in the main policy for this role) from their personal twitter accounts, and this guidance does not cover or affect Members' personal use of twitter for personal and domestic tweets in any way.

1.6. Skype and other video messaging services

Skype and other video messaging services may be useful tools for Members to communicate with residents and service users in their ward councillor role, particularly where there are logistical problems in physically meeting. As the caller can be viewed and therefore their identity verified, personal information including sensitive personal information can be discussed with them. There is no record of the conversation so no risks of written communications going astray. This method also allows Members to have face to face meetings with members of the public at convenient or 'out of hours' times whilst minimising the risks to personal safety of Members in visiting people in their homes.

However there are special point to be aware of when video messaging.

- Members should ensure that there is appropriate privacy for both callers and that there is no one overhearing who should not be listening to the conversation.

- Members should be aware of their surroundings. Ensure the video does not capture people talking in the background, so people at the other end of the call cannot lip read what is being said by people not in the call.

- Members should be aware of information in the background of the screen – ensuring that papers etc which are confidential or relate to another person or the Member's personal or work affairs are out of sight. Members are advised to ensure that the screen is angled so that personal information is not visible, especially if the councillor is calling from their home, to prevent unwarranted intrusion into the councillor's home.