MEETING

GENERAL FUNCTIONS COMMITTEE

DATE AND TIME

WEDNESDAY 11TH NOVEMBER, 2015

AT 7.00 PM

VENUE

HENDON TOWN HALL, THE BURROUGHS, LONDON NW4 4BQ

Dear Councillors,

Please find enclosed additional papers relating to the following items for the above mentioned meeting which were not available at the time of collation of the agenda.

Item No	Title of Report	Pages
9.	COMMUNICATIONS WITH THE PUBLIC BY TEXT AND SOCIAL MEDIA POLICY (COUNCIL STAFF)	1 - 12

Sarah Koniarski 020 8359 7574 sarah.koniarski@barnet.gov.uk

This page is intentionally left blank

AGENDA ITEM 9

General Functions Committee

11 November 2015

Title	**Communications with the Public by Text and Social Media Policy for Staff**
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 Policy
Officer Contact Details	Victoria Blyth, victoria.blyth@barnet.gov.uk, 020 8359 2015

Summary

This report asks the Committee to note and comment on the Communications with the Public by Text and Social Media Policy which is in place for staff.

Recommendation

1. **That the Committee note and comment on the Communications with the Public by Text and Social Media Policy which is in place for staff.**

1. WHY THIS REPORT IS NEEDED

1.1 Following consideration of this policy at the last General Functions Committee meeting, the committee suggested that reference to 'Barnet councillors' should be removed from the scope of the policy (page 7) to maintain a clear delineation in its application.

1.2 The Information Strategy Manager was requested to present a further report incorporating the committee's recommendations at the November General Functions Committee meeting. The policy attached as Appendix A to this report has been amended to remove reference to 'Barnet Councillors' in line with the committee's recommendation.

1.3 The 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.

1.4 There have been no reported incidents in relation to the obligations in this policy since it was introduced early in 2015.

2. REASONS FOR RECOMMENDATION

2.1 The General Functions Committee is responsible for all other Council functions that are not reserved to Full Council. The Committee has requested that the amended policy, attached as Appendix A, be presented at its November meeting.

3. ALTERNATIVE OPTIONS CONSIDERED AND NOT RECOMMENDED

3.1 None

4. POST DECISION IMPLEMENTATION

4.1 The Information Strategy Manager will upload the amended policy to the council's intranet and website: Communications with the Public by Text and Social Media Policy.

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.

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

APPENDIX A

Communications with the Public by Text and Social Media Policy

London Borough of Barnet

POLICY NAME	Communications with the public by text and social media policy.		
Document Description	Policy which provides guidance on how to safeguard personal data when communicating with the public through text, IM and other social media methods.		
Document Author 1) Team and 2) Officer and contact details	1) Information Management Team 2) Sarah Laws, Sarah.laws@barnet.gov.uk, ext 2587		
Status (Live/ Draft/ Withdrawn)	Draft	**Version**	01.10
Last Review Date	October 2015	**Next Review Due Date**	October 2017
Approval Chain:	Head of Information Management	**Date Approved**	February 2015

Contents

1. Introduction

In our modern society people wish to communicate with the council in many different ways. Whilst many still communicate by traditional letter, telephone or email, many others wish to use more modern methods. These include (but are not limited to) the familiar and well established such as text message, or more innovative methods such as instant messaging services (eg BBM, IM, What's App etc) or twitter, Facebook, Skype etc. In this policy we refer to all of these methods as "social media".

It is important for the council to allow people to use the most appropriate method to deal with us. This includes communications going from the council to the public by social media methods. When using these social media ways of communication it is important that proper care is taken to ensure that personal data is handled properly.

2. Purpose

This policy explains how data protection standards and duties can be maintained with social media communications where personal data is being communicated by the council. Personal data is explained in 5 below.

This policy does not cover communications for publicity and press purposes or for general use where personal data is not involved. For guidance on those uses of social media please see the council's Social Media Policy

This policy needs to be read in conjunction with the council's other Information Management Policies available here. For example the Records Retention and Disposal Policy apply to social media communications in the same way as paper copies.

3. Scope

This policy covers everyone who works in or on behalf of and who communicate with the public by social media methods. It covers Barnet council employees (permanent, temporary, contractors etc), and employees /contractors /temporary staff in CSG, Re and other delivery units who are working on Barnet work. These people are termed "everyone" in the Policy.

This policy does not apply to Barnet councillors; there is an appendix in the Members' Information Management Policy which covers communications with the public by text and social media by councillors.

4. Responsibilities

Everyone (see 3 above) must comply with this policy.

Non-compliance with this policy may lead to the council breaching the Data Protection Act 1998. Where this occurs disciplinary action may be taken by the

council, and in serious cases may result in criminal prosecutions by the Information Commissioner's Office. Data protection is explained in section 5 below.

5. Personal Data and the Data Protection Act

The Data Protection Act 1998 ("DPA") defines **personal data** as information which relates to a living individual (data subject) who can be identified from those data or from those data and other information which is the possession of, or is likely to come into the possession of, the data controller. This includes information such as name, address, date of birth etc.

Sensitive Personal Data is personal data about the racial or ethnic origin of the data subject, his political opinions, religious or similar beliefs, trade union membership, physical/mental condition, sexual life, commission (or allegations) of an offence or proceedings relating to an offence.

The DPA sets out principles which must be followed when processing personal data. Processing includes obtaining, recording, or holding the data or carrying out any operation or set of operations on the data, including: organising, adapting, altering, retrieving, consulting, using, transmitting, disseminating, making available, aligning, combining, blocking erasing or destroying the data. Therefore it includes communicating with the data subject or any other person by social media methods when personal data (and sensitive personal data) is involved.

The data protection principles and much detailed DPA guidance are set out in the council's Data Protection Policy and the Data Protection Act Compliance Toolkit. They are both available here and must be read and understood by everyone.

Where social media communications which contain personal or sensitive personal data are sent to the wrong recipient this is a breach of the DPA. The council takes all such incidents very seriously and investigates each one. All data incidents (included suspected ones) must be reported to the council. The Security and Data Protection Incident Management Policy sets out how to do this, and there is also a Quick Guide on this area. They are both available here

6. Guidance on Communicating with the Public by Social Media

6.1. General points

The 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.

It is impossible to provide guidance on how to deal with every possible situation, especially in a technologically fast moving and innovative sector. Some general guidance and examples are provided.

In all cases everyone is expected to apply common sense to communications and to take a moment to consider whether what they are doing is sensible and appropriate.

If in doubt, do not send the communication but ask for guidance – in the first instance from your manager or team leader. If they are unsure then your service Link Officer should be able to assist, but if not then ask the Information Management Team for advice, before sending the social media communication. See section 8 for how to contact us.

All communications with the public by social media must be on council issued/approved devices. See the Acceptable Use policy for more details of these devices. Staff members' personal devices should not be used to communicate with members of the public.

6.2. Permission.

When you first begin to deal with a member of the public they will usually give you their preferred contact details. This will be the method you generally use to contact them. They may also give you alternative contact details eg a mobile number or a Skype name. If you are going to contact them by a social media method you have not used before make sure you have their permission to use that social media method.

Don't assume that because someone who usually emails you but has given you their mobile number will want to receive text messages from the council. If you wish to text them ask them whether this is acceptable to them, ensuring you do not put undue pressure on them. If they agree make a note of it on the file.

- For example, a social worker dealing with a young person may usually communicate by text message but the young person mentions that they prefer What's App (for example) as it uses Wi-Fi and doesn't count towards their text allowances. Before communicating via this method the social worker should check that the young person wishes to communicate in this way, ensure they have the correct user name and note this on the file.

6.3. Correct Contact Details

It is vital to ensure you have the correct contact details for the social media method. 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.

- For example do not assume for example that a Mr Andrew Travers' Skype name is AndrewTravers, it could be ATravers321, TraversAofBarnet or any other name. AndrewTravers could be someone else entirely on Skype.

For mobile phone numbers double check that you have all the digits in the correct order, and the right number of digits.

If you have not used that particular communication method before send a test message asking the recipient to contact you by phone. 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 its Jane Bloggs from Barnet Council, I need to contact you, could you please call me on 0208359xxxx thanks.”

6.4. Minimise Personal Data Sent

Social media messaging is not always as secure as other methods and mobile devices are targets for thieves. Texts and other IM messages on mobile phones/devices may be read by others accidentally or deliberately. Therefore to reduce the risks of personal information going astray you should keep the amount of personal information in social media messages to the minimum required. This is especially important with sensitive personal information.

- For example instead of saying in a What’s App message “Hello Jane Bloggs, I’m confirming that Sheela Patel the child protection social worker will meet you on Thursday 20th January at 2.30pm at your house 3 Any Street to discuss why your son Basil is on the child protection register”

  You could say “I’m confirming our meeting at your house on Tuesday 20th Jan at 2.30pm. If you’re not sure why we are meeting please call me. Sheela Patel, Barnet Council.

- For example instead of saying to a young person in care “Hi Phil, we will have our looked after child review next Wednesday after school, in the welfare room at East Barnet School, Donald, Children’s Services”

  You could say “Hi Phil, wanted to remind you we are meeting in the school office after school on Wednesday, Donald, Barnet Council”

Reducing the amount of sensitive personal data to an absolute minimum is also important. 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 should be used in preference to text or other IM services, as it is as quick but a more secure format. Where contact does need to be made through social media, especially where this is the way of communicating a message requesting contact should be made instead of sending sensitive personal information.

- For example instead of a Facebook message saying “I need to discuss an issue with your mum Ethel, as we are concerned that her relationship with Barnaby in the care home is inappropriate, given they are both over 90 and have dementia, and we don’t think either of them have capacity to consent to a physical relationship”

- You could say “Please can you call me on 0208359xxxx to discuss an issue with your mum that we can’t do over Facebook. It’s urgent but nothing to panic about, thanks.”

The messages need to give enough information to inform without imparting too much personal detail. It is important not to be too vague as this can cause alarm.

- A true life example of this would be a text from a Barnet school to a parent which stated “Please can you call the school urgently about your child” resulting in a panicked parent ringing the school, not knowing which child was either in serious trouble or being rushed to hospital, to find that it was a routine chaser about a non-payment for a school trip.

- It could have said “Please can you call the school about a payment”

6.5. Twitter

The council has a twitter account and the use of this is covered by the council’s Social Media Policy. This account must not be used to tweet personal information.

It may be that a resident sends a direct message containing personal information through twitter to the council’s twitter account. A direct message should be sent to them requesting that they contact the council and ask for a named person on a given contact number. It is important to ensure that the correct user is selected, that a direct message is selected not a public tweet and no personal information is given in the message.

6.6. Skype and other video messaging services

Skype and other video messaging services may be useful tools for communicating with residents and service users, 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.

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

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

- Be aware of your 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.

- Be aware of information in the background of the screen – ensure that papers etc which are confidential or relate to another person are put away, and that the screen is angled so that personal information on other people's desks is not visible.

- Video conferencing is not the same as a face to face meeting and if bad/ unwelcome or difficult news is to be given or discussed it might be better to do this face to face. Service areas should have their own guidelines for these service specific situations.

6.7. Consequences of sending personal data to wrong contact details

The consequence of sending personal information to the wrong person is that a data breach will have been committed. In some cases this will cause only inconvenience and delay; however in other cases they can have very serious consequences for data subjects. The council takes **all** data protection incidents seriously, as explained in section 5 above. All incidents or suspected incidents need to be reported immediately, as set out in the Security and Data Protection Incident Management Policy available here

7. Review of the Policy

This policy and guidance will be reviewed annually or earlier as required by policy or legislation changes.

8. Contact Information/Further Guidance

Further advice and guidance is available from the Information Management Team:

Information Management Team:

Tel 020 8359 7080

Data.protection@barnet.gov.uk