## Introduction

Members have both rights and responsibilities when it comes to accessing and handling information, especially personal information about individuals. These rights and responsibilities fall under a variety of legislation, council policy and common law.

As Members of the Council, councillors have duties to ensure that the London Borough of Barnet meets its statutory obligations about handling information. In addition, they are individually responsible and liable to legal action under data protection legislation for some of the information they handle about individuals.

## How this Toolkit works

This toolkit sits beneath the Members' Information Management Policy and sets out rights and responsibilities of Members, and officers when sharing or disclosing information to Members.

## Contents

# 1. Freedom of Information

## 1.1. Requests to the council

The Freedom of Information Act 2000 (FOIA) provides a right of access to information held by a public authority. The Environmental Information Regulations 2004 (EIR) also provides a right of access to information but more specifically deal with environmental information. When we refer to FOI / FOIA we are including EIR.

In their role as a Member of the Council, information held by Members is subject to the FOIA and may be disclosed, unless an exemption applies. For example, emails between a councillor and an officer in relation to a report to a committee or a policy would be covered by the FOIA and therefore subject to disclosure.

The council has a commitment to transparency and openness and information is regularly and routinely released under FOIA. This includes correspondence between Members and officers where it is required to release under FOIA.

Members may receive requests from the Information Management Team or from FOIA link officers across the council asking if they have any information that relates to an FOI request. Members are obliged by law to provide any relevant information that they hold. If a Member believes that a valid FOI exemption may apply, they must still provide the information, but advise the officer why it is thought that an exemption may apply. Failure to provide information for a valid FOI request is a breach of the legislation.

Information that Members hold in their role of ward representative or as a member of a political party is not covered by the FOIA and is therefore not subject to disclosure, even if it is held on Barnet Council systems. This is because the council is holding information 'on their behalf' and it is not managed or controlled by the council. For example, an email between a councillor and a resident about a problem they have asked for help with would not be covered by FOIA, even if held on a Member's Barnet email account.

If a Member receives a request for information held by the council, this must be passed to the council's Information Management Team foi@barnet.gov.uk as soon as possible. The council is legally required to respond to a request for information promptly and no later than 20 working days after the request was made. Failure to respond within the proscribed timetable can lead to complaints to, and investigations and monitoring by, the ICO.

More detailed information on FOIA and EIR is available in the council's Public Access to Information Policy.

### 1.2. Helping a resident make an FOI request

An FOI request must be in writing and must give the name of the requester and a clear description of the information that they are requesting. The council has an FOI request form on its website or a request can be made by email to foi@barnet.gov.uk

The ICO website has detailed information on making an FOI request and what exemptions apply.

## 2 Data Protection Act (DPA) Requests

Data subjects (individuals) have rights under data protection legislation to how their information is processed.

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Rights related to automated decision making and profiling

More information on each of these rights can be found in the council's data protection policies or on the ICO website.

### 2.1 Requests by individuals for their own information

The 'right of access' allows individuals to access their own information. These requests are known as Subject Access Requests (SARs). Requests can be made for information held by the council, which includes Members acting in their role as a Member of the Council.

Members are considered individual Data Controllers in their own right, for personal information they hold in their role as ward representative.

The DPA requires that information must be provided promptly and within a calendar month (30 days), unless any exemptions listed in the DPA apply.

### 2.2 Requests of the council

Members will not routinely be asked if they hold information about individuals. However, if an individual makes a SAR where the scope of the enquiry may cover

personal information held by a Member during their work for the council, the Information Management Team or a service link officer may ask a Member to search their paper and electronic records.

Information should only be provided where it is held by the councillor in their role of Member of the Council, and not in their role as ward representative or political party member.

### 2.3 Requests for information held by a Member

If a Member receives a request from an individual asking for their own information the Member needs to determine whether the individual is asking for information held by the Member acting as a ward representative, or whether they are asking for information held by the council. If it is a request to the council the Member should forward this immediately to the Information Management Team data.protection@barnet.gov.uk

**Example:** "I would like to see all information the council holds about my renting an allotment"

If the Member holds any information in their role as Member of the Council, they should provide this to the Information Management Team at the same time as passing on the request.

If the Member determines that it is a request to them in their role as ward representative, they are responsible for responding to it in an appropriate manner under the legislation.

**Example:** "I would like to see a copy of all emails you have sent about me when helping me rent my allotment."

The ICO has guidance on how to respond to a SAR. Additionally, the Information Management Team can provide advice, although the Member remains individually responsible for handling the request.

## 3 Members' access to information

By nature of being an elected representative, Members have access to a large amount of information that is not publicly available or where public awareness is such that an FOI request is unlikely. The sections below provide information on how Members can access information that they are entitled to. Personal data (as defined by legislation) should only be provided to Members by council officers in a secure manner, especially where the data is more sensitive and is considered 'special category' data. Members should use their LB Barnet email accounts for this purpose and officers should only provide personal data to Members by using the Member's official account, unless the officer has the approval of the data subjects concerned, or of the Information Management Team, to use another route.

### 3.1 Access to information contained in committee papers

The council's Access to Information Procedure Rules, part of the council's Constitution, details the rights of Members to access documents associated with committee meetings. These rules relate specifically to information concerning meetings of the Council and cover rights established under the Local Government Act 1972 (as amended), among others. Members have a general right of access to all information classified as exempt in committee reports except in some exceptional circumstances (such as reports relating to Member conduct complaints being considered by the Group Leaders Panel).

### 3.2 Access to information not contained in committee papers

Establishing a 'need to know'

For access to information and documents which are not contained in committee papers Members have the right to request information where they can show a reasonable 'need to know' that information to perform their duties as a councillor. Access to information in this way is a common law right which has been confirmed in case law. When requesting access to non-committee information, Members should provide information supporting the reasons that they need to know the information requested. Members have a duty to fully demonstrate their need to know when requesting personal information about an individual.

In many circumstances, a Member's 'need to know' will be presumed, such as a committee member wishing to inspect documents or briefings relating to the functions of that committee. However, the law does not allow a 'roving commission' and in some circumstances, such as when requesting personal information about individuals, or information that might be considered commercially sensitive or business confidential in some way, the motive for requesting information will be relevant and a Member will be expected to justify their request for information.

### 3.3 Requesting non-committee information and assessing the 'need to know'

Members can request information through the Member Enquiry Service. The request for information should also provide evidence supporting the Member's need to know that information. This is especially true for personal data. Where the service area is satisfied that a reasonable 'need to know' has been demonstrated by the Member, the information will be released. If the service area considers that the reasonable 'need to know' has not been demonstrated and the information should not be released they should seek advice from the Information Management Team before finalising that decision.

Should a Member be dissatisfied with the response they receive (for example if access to information is refused or partly refused), they may wish to resolve this informally with the relevant Head of Service. Alternatively, they may contact the council's SIRO (Senior Information Risk Owner).

### 3.4 Appeal against a decision to not disclose non-committee information

Members should email or meet with the SIRO to explain what information they have requested, what the response has been, why they are dissatisfied and the reasons for wishing to access the information. A form with guidance is available at Appendix A. The SIRO will investigate the matter, considering the representations made by the Member, and discuss with the Data Protection Officer (DPO). The SIRO will decide whether the requested information can be provided to the Member, and whether any redactions should be made to enable more information to be provided.

Should the SIRO form the opinion that the Member concerned does not have the 'need to know' or for some other reason, that decision will be reported to the Chief Executive, who will review the SIRO's decision.

Should the Member concerned disagree with the findings of the Chief Executive then they shall have the right to have their request heard by the Constitution and General Purposes Committee.

### 3.5 Members' interests and non-committee information

Members should not ask for information on a matter which would personally affect them, in which they are professionally interested or where they have a pecuniary interest as set out in the Code of Conduct for Members in the council's constitution. Members can seek guidance from the Monitoring Officer on matters where they consider they might have a pecuniary or non-pecuniary interest.

### 3.6 Distribution of non-committee information

Guidance on confidentiality is provided in section 4 of this toolkit.

### 3.7 Members' rights to make Freedom of Information requests

Members are reminded of their ability to make a Freedom of Information (FOI) request.

### 3.8 Local Authority Accounts

The Audit Commission Act 1998 sections 14-16, and the Accounts and Audit (England) Regulations 2011 Regs 21, 22 and 25 provide a right to inspect the council's accounts, take copies of documents and question the auditor. These rights are available to everyone – members of the public and Members alike. The rights to access documents are restricted to prevent access to personal information and to information considered to be commercially sensitive. Requests to access information under these rights should be made to the council's Director of Resources.

Members may be able to gain access to information restricted under the Audit Commission Act under their common law right of access as detailed in para 2.28 above. When accessing information that would be withheld from the public under

the Audit Commission Act right of access, members are reminded of their obligations under the Members' Code of Conduct not to disclose this information to third parties.

### 3.9 Member Enquiry Service

The Member Enquiry Service is the central point of contact for Members to submit requests for information from the council. There is a central Member Enquiry Team (MET) within Customer Services who log, route, track and chase each request from a Member.

Members can request information by:

- contacting the MET on 020 8359 2002
- emailing members.enquiries@barnet.gov.uk
- emailing their preferred contact in any service with a cc to members.enquiries@barnet.gov.uk

### 3.10 Member FOI Requests

Members have the same rights as anyone to make a request under FOIA. However, as a release of information under FOIA is a release of information to the public at large, a request from a Member is treated the same as if it were from a member of the public.

As Members may have access to more information than members of the public they may find that using the Members Enquiry Service is a more appropriate route than making a FOI request. A FOI request will give them the same information as a member of the public would receive, as FOI responses are publicly available documents.

Occasionally there may be situations where Members wish to know how much information would be publicly available in respect of a particular issue and so may wish to make a FOI request.

## 4 Confidentiality

### 4.1 Right to Make Public

The right of access is not the same as the right to publish or make public. As per the Members Code of Conduct:

You must not:

> (a) 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, except where:
>
> > (i) you have the consent of a person authorised to give it;

(ii) you are required by law to do so.

If a Member intends to refer to conclusions reached from having read confidential or exempt material, they may wish to consult with the Monitoring Officer or Information Management Team for guidance to prevent the unintentional disclosure of that information.

Disclosing confidential information may be considered a breach of the Members Code of Conduct. If a Member believes that the disclosure of confidential information is necessary for the effective performance of their duties as a Member they should seek advice from the Chief Executive or the Monitoring Officer. This should be undertaken prior to any disclosure being made.

Information released through an FOI request or information published on the council's website as part of the committee process are in the public domain and therefore may be shared with others.

## 5 Data Protection

Personal information held by Members on behalf of the council must be handled appropriately and kept secure. This section has guidance on how to do this. Disclosing personal information inappropriately or handling it poorly would leave the council liable to action under the law and by the ICO.

Personal information held by Members as ward representatives is the responsibility of the individual Member. As a data controller, each Member is responsible to ensure appropriate processing and security of the information. Disclosing personal information inappropriately, or refusing to disclose information when required by law are likely to be a breach of the Members Code of Conduct and, where there is a breach of the DPA, it is likely to be an offence for which a Member is personally liable.

Data subjects (individuals) are entitled to complain to the ICO if they feel a data controller has not complied with their obligations under data protection legislation. The ICO will investigate and may take enforcement action or issue a fine.

### 5.1 Personal data

Personal data is defined as any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This means information about an individual's personal or family life and business or profession life. Format does not matter as personal data may be paper, electronic, emails, photographs, verbal information or identifiers like IP address, case reference number or NHS number.

Special category data is more sensitive personal data about:

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic and biometric data for purpose of uniquely identifying someone
- Health
- Sex life or sexual orientation

Personal data relating to criminal convictions & offences is covered by separate legislation but broadly, should be treated carefully, as with special category data.

A higher level of security and care should be applied to special category or criminal data.

### 5.2 Record of Processing Activity (ROPA)

Each data controller is required to keep a Record of Processing Activity (ROPA). The council holds and maintains a ROPA for the processing that it undertakes on its own behalf, and on behalf of others.

Members must keep a ROPA which contains:

- The name and contact details of the data controller (the Member)
- The purposes of your processing
- A description of the categories of individuals and categories of personal data
- The categories of recipients of personal data
- Details of your transfers to third countries including documenting the transfer mechanism safeguards in place
- Retention schedules
- A description of your technical and organisational security measures

Guidance on a ROPA template can be obtained by contacting the Information Management Team.

### 5.3 Passing on Information from Constituents

Where a constituent has contacted a Member directly, they are usually doing so in a Member's capacity as their elected ward representative. Members are therefore acting in their own right, not on behalf of the council, and Members are responsible as data controllers for the handling of that information.

When requesting information or action from the council on behalf of a resident a Member should only forward the minimum details necessary for the issue to be dealt with and not, for example, an entire letter or email chain. It may also not be relevant

to disclose the identity of the resident. Alternatively, Members may ask the constituent's permission to pass on information or correspondence. This is especially true where special category data is concerned.

It is important that special care is taking when disclosing or sharing sensitive personal information. If the person's express consent has not been obtained to disclose or share, and Members are unsure whether the disclosure or sharing would be necessary or appropriate, advice should be sought from the Information Management Team prior to disclosure to ensure that the disclosure is legal.

### 5.4 Handling of Records

It is recognised that the majority of confidential or personal information handled by Members will be in their own homes, rather than a council office environment. However, information must be held and transported securely. A loss of personal information is a breach of the DPA, and may lead to action against the council or the Member.

## 6 Access to council systems and information

Only corporately managed machines (computers and mobile equipment such as phones and tablet devices) may be used to access the council network and its systems and / or to work on council information. The network can be accessed from a home broadband or public Wi-Fi via Citrix or VPN, or through Blackberry and Mobile Iron technology on phones and tablet devices.

Users should not attempt to access the council's network from privately owned devices as this puts the council's network at risk. In emergency situations where business continuity plans are brought into effect, these rules may be relaxed. These situations will be notified to members when they occur by the Members IT Support Team.

Giving access to corporately managed computers and mobile equipment such as phones and tablet devices to anyone except the council IT department is not allowed. More information can be found in the council's Acceptable Use Policy.

### 6.1 Access to the network when overseas

If a situation arises in which Members need to take their device out of the UK they must first check with the Members IT Support service (020 8359 3333) membersICTsupport@barnet.gov.uk, as it may put council information and the council network at risk. Some countries are barred from connecting to Public Services Network connected networks. Certain countries may also confiscate encrypted devices on entry and/or force a user to enter passwords and bypass security. Confiscated devices may not be returned on exit in all cases. Please contact the Members IT Support service if you need to work outside the UK and

have to have roaming enabled on your device. Members are requested to use wi-fi wherever available.

### 6.2 Requirements for Safe Handling of Council Information

Confidential council information and personal information about individuals should be held securely both when in use, and when stored away, whether at a council building or in the home/work place of a Member. Encrypted council equipment should be used for electronic records and paper records should be stored and transported securely.

The following are best practice guidelines on how to handle information appropriately:

- Don't carry paper records 'loosely' as this increases the risk of dropping or losing them, or that they come loose from the rest of the file.
- Don't carry paper records/ in the same bag as your tablet or in any other bag containing valuables, as these are often the primary target for thieves.
- Because valuable items in a Member's home may be a primary target for thieves, council paper records should be kept separately from valuable items. Ensure electronic equipment has the encryption engaged during travel by turning off the tablet or laptop.
- Ensure paper records are not in transit or away from your main place of work for any longer than is necessary. They should be delivered to their destination at the earliest opportunity, or returned to your main place of work promptly.
- Don't leave bags or cases containing paper files or electronic equipment visible in a car; if it is unavoidable to leave items in a car, lock them in the boot or glove compartment. eg whilst filling up with petrol.
- When travelling on public transport keep your bag/case containing paper records close by at all times. Items should not be placed in luggage racks or storage areas, as this increases the possibility of theft or the misplacing of the item.
- Paper records should only be transported for necessity and not for convenience. Where paper records have to be taken away from or transported between the office or home environment, only the minimum amount of personal or other confidential data necessary for the job in hand should be removed and, where possible, data should be anonymised.
- It is good practice to keep a record of what information you are transporting so that an appropriate risk assessment can be done in case of loss.

- When collecting information the same considerations should be taken, and the information appropriately protected at all times.

Any loss of personal or confidential information must be reported to the Information Management Team by emailing data.protection@barnet.gov.uk The team will assess the incident in line with the council's data protection and information security policies.

Legislation requires that data protection and security incidents meeting criteria are reported to the ICO within 72 hours. It is therefore very important that potential incidents are reported as soon as the Member becomes aware of them.

### 6.3 Constituency Information

Members are responsible for keeping personal information relating to their ward constituency work secure and in line with the Principles of the DPA. Guidance is available on the ICO website. Whilst responsibility remains with the Member, they may wish to follow the guidance provided for council information for their own constituency records as well.

In the event of a loss of constituency personal information, Members are responsible for this and should refer to the ICO's guidance on losing personal data.

### 6.4 Loss of equipment or information

The loss of a council owned device, such as tablet or BlackBerry, must immediately be reported to the:

Members' IT Support on 020 8359 3333 or membersICTsupport@barnet.gov.uk

Insurance team on 020 8359 7197

The loss of any council information should be reported to the Information Management Team as above.

Timeliness of reporting is key to ensure measures are put in place to contain and mitigate any security risks or data loss.

## 7 Records Retention

### 7.1 General Principles

Members will collect a lot of information as part of their duties. It is recommended that Members create appropriate storage to ensure that information relating to their three roles as an elected representative is kept separate.

It is a requirement of the DPA that personal data should only be retained for as long as it is required for the purpose it is submitted. It is also a requirement for it to be accurate and up to date, kept and disposed of securely (eg shredded if in paper format).

It is not permissible to keep personal information 'just in case' or to use it for a different purpose than it was originally given. The ICO has detailed guidance.

### 7.2 Information relating to council business

This is information generated by officers or Members in relation to work for the council or on behalf of the council. Examples of these records are minutes, agendas, or any document issued by the council.

The relevant service area is responsible for keeping these records in line with council policy. Members should therefore only keep this information for as long as they require it.

However, if a Member is unsure if the council holds a document and retains it as a record, they should check with the relevant service before they dispose of it.

### 7.3 Constituency information

Information relating to a Member's work as a ward representative is between the Member and their constituent and the Member is personally responsible for its safekeeping and appropriate handling. This information will inevitably contain personal data, so the principles of the DPA must be abided by.

Personal information should only be kept as long as necessary, only used for the purpose it was originally given, and disposed of securely.

### 7.4 Information relating to political beliefs

If a Member is affiliated to a political party then they will have information that relates to party business; these records should be dealt with in accordance with advice from the party in question.

## 8 Advice for Officers

It is important to note that whilst Members have the right of access to a wide range of council information, there is not an automatic right to all information or to personal information about individuals. Officers should ensure that they have consent of the data subjects concerned or an appropriate legal basis for disclosing the information to a Member. In addition, it is the responsibility of the officer providing the information to make the Member aware of what they can do with the information. For example, personal information provided so that a Member can respond to a constituent's request for help, must only be used for that purpose.

If an officer is in doubt about what information should be supplied, advice must be sought from the Information Management Team and the Data Protection Officer.

Personal data should only be sent to a Member's official council email address. This is because it is the council's responsibility to disclose information in a secure manner. If a Member has contacted the officer from a different email address, the response should still be sent to the official email account, and it is courteous for the

officer to let the Member know that this has been done. Non-Barnet email accounts may be used for requests for meetings between Members and officers and similar such requests not involving resident/client personal information.

All Members enquiries should be responded to promptly. Regardless of who receives the query in any service area, it should be sent immediately to the relevant Member Enquiry Link Officer for each service area/department to coordinate, and copied to members.enquiries@barnet.gov.uk.

## 9 Communicating with the Public by Text and Social Media for Members

When acting as a Member of the Council this guidance must be followed to ensure that the council is abiding by the DPA. It does not formally apply when a Member is acting in their capacity as a ward representative or in their role representing a political party, as these are not the responsibility of the council. However, Members may find this guidance a useful reference in helping them meet their individual data protection responsibilities when acting as ward representatives or political party member.

The public wish to communicate with their councillors in many ways. Whilst many still communicate by traditional letter, telephone or email, others wish to use social media. These include (but are not limited to) text message, instant messaging services like What's App or twitter, Facebook, Skype etc. In this toolkit 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 ones.

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 with them.

### 9.1 General points

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 and the same common sense rules apply. The more informal nature of social media can 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.

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 Member of the Council 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. They can of course be used for political communications.

### 9.2 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.

**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.

### 9.3 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.

**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."

### 9.4 Minimise personal data sent

Social media messaging is not 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 more sensitive personal information such as special category personal data for financial information.

**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"

### 9.5 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.

### 9.6 Skype and other video messaging

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 meeting in person. As the caller can be viewed and therefore their identity verified, personal information including Special category 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.

## Appendix A – Member's Referral to SIRO

**GUIDANCE NOTES**

2 *Councillor's email and telephone number*. Please provide your Barnet email address and your preferred telephone number.

3 *Service holding information requested.* Team and if possible named individual, as the more detail given will make the process more efficient.

4 *Description of Information requested*. Please be as specific as possible. If you have an email that was sent to the service please attach this.

5 *Councillor's reasons for requesting information.* Please set out as fully as possible the reason for wishing to have this information, for example relating it to work of a committee upon which you sit, or case work you are involved in. If it involves personal information of third parties it would be helpful if you could provide their consent for you to see the information.

6 *Response provided by the service*. Please attach any emails if you have them, or if not please provide a précis of their response.

7 *Reasons for the councillor's dissatisfaction with the response provided by the Delivery Unit.* Please explain why you are dissatisfied with their response; relating your reasons to the information you gave in 5 above would be very helpful.

**Guidance Notes for SIRO Decision**

The SIRO will review the request with the Data Protection Officer, and may need to consult with the Director or Head of Service or other colleagues in the service. An informal resolution is always encouraged. The SIRO may need to consult with specialist officers as required by the subject matter, these could include the Caldicott Guardian, the Monitoring Officer, lawyers at HBPL or others as required.

The SIRO will keep a record of the persons consulted and the SIRO's decision, which will be provided to the Chief Executive.

**Member's Referral to SIRO**

Complete this form and send it, with any relevant attachments, to the SIRO.

| | |
|---|---|
| 1 | Name of Councillor: |
| 2 | Councillor's email and telephone number |
| 3 | Service holding information requested (incl team and if possible named individual) |
| 4 | Description of Information requested |
| 5 | Councillor's reasons for requesting information (please be as specific as possible) |
| 6 | Response provided by the service |
| 7 | Reasons for the councillor's dissatisfaction with the response provided by the service |



**Document Control**

| | | | |
|---|---|---|---|
| **TOOLKIT NAME** | Members' Information Management Toolkit | | |
| **Document Description** | Toolkit complements the Members' Information Management Policy and provides practical guidance on handling personal data. | | |
| **Document Author**<br>1) Team and<br>2) Officer and contact details | 1) Information Management Team<br>2) Victoria Blyth, victoria.blyth@barnet.gov.uk | | |
| **Status**<br>(Live/ Draft/ Withdrawn) | Live | **Version** | V01.1 |
| **Last Review Date** | | **Next Review Due Date** | July 2020 |
| **Approval Chain:** | Data Protection Officer | **Date Approved** | July 2018 |

**Version Control**

| Version number | Date | Author | Reason for New Version |
|---|---|---|---|
| V.001 | 03/05/2018 | Victoria Blyth | Initial draft |
| V01.0 | 04/05/18 | Victoria Blyth | Creation of document in new policy framework, to complement Member's Information Management Policy |
| V01.1 | 06/07/2018 | Victoria Blyth | Clarification on use of official email accounts for sending and receiving personal data. |