BARNET
LONDON BOROUGH

Appendix 1

Members' Information Management Policy

London Borough of Barnet

Document Name	Members' Information Management Policy		
Document Description	Document which provides guidance for members and others on councillors' right to access information, and how requests should be handled and provides best practice advice.		
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Status (Live/ Draft/ Withdrawn)	Draft.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**	02.04
Last Review Date	March 2014	**Next Review Due Date**	n/a (draft)
Approval Chain:	GFC	**Date Approved**	n/a (draft)

Version Control

Version number	Date	Author	Reason for New Version
V1	Mar 2014	V Blyth	Policy creation
V1.1	Nov 2014	S Laws	Proposed amendments taking into account changes in constitution and methodology for dealing Members requests for information
02.03	December 2014	Sarah Laws	Incorporating comments from others, IMGGs and comms
02.04	Jan 2015	Sarah Laws	Amended following discussions with governance and councillor

Contents

1. Introduction

Members of the Council 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 with regard to handling information. In addition, they are individually responsible and liable to legal action under the Data Protection Act 1998 for some of the information they handle about individuals.

2. Purpose and scope

The purpose of this policy is to provide Members with information about their rights to access information, the rights of individuals to access information held by the council and individually by Members, and requirements on Members for how to handle information.

This policy includes the good practice standards recognised by the Information Commissioner's Office (ICO). The Information Commissioner is responsible for administering the provisions of the Data Protection Act 1998 (DPA), The Freedom of Information Act 2000 (FOIA) and other information legislation. The ICO has powers to take legal action against organisations or individuals, including Members, found to be acting in breach of the DPA or other information legislation.

The policy is also relevant for officers of the council to understand what information Members are entitled to access and any actions required to be undertaken by the council when providing information to Members.

3. The role of the elected Member

In terms of information legislation, elected Members of a local authority are considered to fulfil three roles:

1. They act as a Member of the Council, for example, as a member of a committee.

2. They act as a representative for residents of their ward.

3. They may represent a political party, especially at election time.

These three roles have different rights of access and different responsibilities under information legislation, which are covered as part of this policy. In addition, the ICO provides a Good Practice Note for elected representatives that Members are encouraged to read.

4. Notification

The DPA requires Data Controllers to 'notify' or register with the ICO. A Data Controller is the person or organisation that determines the manner in which personal data is processed, such as what is collected, what is done with it, how it is stored and when it is deleted or disposed of.

The council registers with the ICO as an organisation and work done by Members in their role as a Member of the Council is covered by that registration.

Members are individually responsible for personal data they manage in their role of ward representative and the ICO requires councillors to register as separate Data Controllers. This is a completely separate notification to any council wide or political party notification.

Whilst many authorities require Members to undertake their own individual registrations with the ICO, Barnet Council undertakes a Member's annual notification to the ICO on their behalf. Members are required to notify the Information Management Team of any changes of name or address in order that the ICO registration can be kept up to date.

5. Freedom of Information requests

5.1. 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. For the purposes of this policy the use of FOI / FOIA is deemed to cover EIR as well.

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 FOI and EIR Policy.

5.2. 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.

6. Data Protection Act (DPA) Requests

6.1. Requests by individuals for their own information

The DPA allows individuals the right 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 40 calendar days, unless any exemptions listed in the DPA apply.

6.2. 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 in the course of 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.

6.3 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.

7. Members' access to information

7.1. 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.

i. **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).

ii. 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 in order 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 will have a particular 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, or a Ward Member requesting information on local matters affecting their ward. 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 to be 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.

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

Members can request information in the ways explained in section 7.3 (Member Enquiry Service). The request for information should also provide evidence supporting the Member's need to know that information. 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 making 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), who is the Deputy Chief Operating Officer. The SIRO is the council's information risk owner.

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. The SIRO will investigate the matter, taking into account the representations made by the Member, and taking expert advice where required from relevant professionals (for example the Monitoring Officer or the

Data Protection Officer etc.). The SIRO, whose view will be final, 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. Decisions taken by the SIRO to not provide information to Members in accordance with this policy will be reported quarterly to the General Functions Committee for information.

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 in respect of which they have a pecuniary interest as set out in the Code of Conduct for Members in the council's constitution. Members are able to seek guidance from the Monitoring Officer on matters where they consider they might have a pecuniary or non-pecuniary interest.

Distribution of non-committee information

Guidance on the further distribution of information pursuant to this paragraph is in section 8 of this policy.

Members' rights to make Freedom of Information requests

Members are reminded of their ability to make a Freedom of Information (FOI) request as detailed in section 7.4 below.

7.2. 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 Deputy Chief Operating Officer.

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 7.1 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.

7.3. 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.

Any enquiries sent through by Members or MPs must be responded to within 5 working days.

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

7.4. 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 (as explained in 7.1 above) they may find that using the Members Enquiry Service as detailed in 7.3 above) will usually be 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 considered to be publically available documents.

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

8. Confidentiality

8.1. Right to Make Public

The right of access is not the same as the right to publish or make public. As per section 4 of 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 is made.

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

9. 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 this 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 under the DPA, 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.

9.1. 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 representative. Members are therefore acting in their own right and not on behalf of the council. As such 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 sensitive personal information is concerned..

Personal data is information which would allow an individual to be identified, such as name, address, telephone number, reference numbers, car registration numbers and such like. The Data Protection Act 1998 section 2 defines "sensitive personal data" as personal information which also is information relating to race or ethnic origin, political opinions, religious or similar beliefs, trade union membership, physical or mental health or condition, sexual life (which includes sexuality) and whether they have committed or are alleged to have committee an offence.

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 Data Protection Act is not inadvertently breached. Sensitive personal information must always be stored in a safe location. Advice is provided in 10.2 below.

The ICO's Good Practice Note provides more information on a Member's responsibilities Handling of Information

9.2 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.

10 Access to council systems and information

Only LBB corporately managed machines (computers and mobile equipment such as phones and tablet devices) may be used to access the LBB 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.

10.1 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 if this is appropriate, 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.

10.2 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 data.protection@barnet.gov.uk who will assess the incident in line with the council's Data Protection and Information Security policies.

10.3 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 by following the link above. Whilst responsibility remains with the Member, they may wish to follow the guidance provided in 10.2 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.

10.4 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.

11 Records Retention

11.1 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 (e.g. shredded if in paper format) in accordance with the council's Records Retention Policy.

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.

11.2 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 the council's Records Retention Policy. Therefore Members should 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.

11.3 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.

As discussed in 11.1, personal information should only be kept as long as necessary, only used for the purpose it was originally given, and disposed of securely.

11.4 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.

12 Advice for Officers

This policy applies when Members are entitled to access information and therefore when it is appropriate for an officer to provide information to a Member.

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. In addition, it is the responsibility of the officer providing the information to make the Member aware of what they are allowed to 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 should be sought from the Information Management Team.

All Members enquiries should be responded to within 5 working days. 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 co-ordinate, and copied to members.enquiries@barnet.gov.uk

13 Contact information / further guidance

The Information Management Team is available to both Members and officers to advise on access to and the proper handling of information.

Address: Information Management Team, London Borough of Barnet
1st Floor, Building 2 North London Business Park
Oakleigh Road South
London N11 1NP

Tel No: (020) 8359 2029
Email: data.protection@barnet.gov.uk or foi@barnet.gov.uk
Website: www.barnet.gov.uk/data-protection-act and on the intranet at this link: https://employeeportal.lbbarnet.local/home/departments-and-services/central-services/information-management/information-management-policies/information-governance-policies.html