Data Protection Act Compliance Toolkit

London Borough of Barnet
**POLICY NAME**

Data Protection Act Compliance Toolkit.

**Document Description**

Document which provides general, more detailed and some specific expert guidance on ensuring compliance with the Data Protection Act.

**Document Author**

1) Team and
2) Officer and contact details

1) Information Management Team
2) Lucy Martin, lucy.martin@barnet.gov.uk ext: 2029

**Status**

(Live/ Draft/ Withdrawn)

Live

**Version**

02.00

**Last Review Date**

March 2015

**Next Review Due Date**

May 2016

**Approval Chain:**

Head of Information Management

**Date Approved**

21 May 2015

**Version control**

<table>
<thead>
<tr>
<th>Version no.</th>
<th>Date</th>
<th>Author</th>
<th>Reason for new version</th>
</tr>
</thead>
<tbody>
<tr>
<td>V01.00</td>
<td>04/01/13</td>
<td>L. Wicks &amp; C McConigley</td>
<td>New Policy</td>
</tr>
<tr>
<td>V01.01</td>
<td>18/10/13</td>
<td>L. Martin</td>
<td>Policy review, including the merging together of the staff guide with the compliance toolkit.</td>
</tr>
<tr>
<td>V02.00</td>
<td>26/02/15</td>
<td>L. Martin</td>
<td>Annual Review. Inclusion of ICO recommendations.</td>
</tr>
</tbody>
</table>
Contents

1. Introduction ...................................................................................................... 5
2. Purpose & scope.............................................................................................. 5
3. Responsibilities ................................................................................................ 5
4. Key definitions.................................................................................................. 6
5. Core guiding principles..................................................................................... 7
5.1. Principle 1 – fairly & lawfully processed ........................................................... 7
5.2. Principle 2 – processed for limited purposes .................................................... 9
5.3. Principle 3 – adequate, relevant and not excessive ......................................... 9
5.4. Principle 4 – accurate and up to date ............................................................. 10
5.5. Principle 5 – not kept longer than is necessary .............................................. 10
5.6. Principle 6 – processed in line with Data Subjects rights ............................... 11
5.7. Principle 7 – keeping information secure ....................................................... 12
5.8. Principle 8 – Personal data not to be transferred to other countries without adequate protection in place ......................................................... 14
6. Project work ................................................................................................... 14
7. Information sharing ........................................................................................ 16
8. Section 29 - Crime and taxation ..................................................................... 17
9. Section 35 – Legal Advice and Proceedings .................................................. 20
10. Data loss / data security incidents .................................................................. 24
11. Communicating with the ICO ......................................................................... 24
12. Data Protection Complaints ........................................................................... 24
APPENDIX A - Schedule 2 & Schedule 3 Conditions ............................................... 25
APPENDIX B - Information Management Impact Assessment ................................. 27
APPENDIX C – Section 29 Requester Template ...................................................... 34
APPENDIX D – Section 35 Requester Template ...................................................... 36
APPENDIX E1 - Due Diligence Security Checklist Template ........................................ 38
APPENDIX E2 - Due Diligence – Evaluation Guidance ............................................. 41
13. Review of the Policy ....................................................................................... 42
14. Contact Information/Further Guidance ........................................................... 42
1. Introduction

The Data Protection Act 1998 is the UK law which governs the way organisations and individuals handle personal data i.e. information that can identify a living individual.

This legislation has eight core principles which must be adopted when handling personal data.

These are: that personal data must:

1. be fairly and lawfully processed
2. be processed for limited purposes
3. be adequate, relevant and not excessive
4. be accurate and up to date
5. not be kept for longer than necessary
6. be processed in line with the rights of individuals under the DPA
7. be kept secure
8. not be transferred to other countries without adequate protection

2. Purpose & scope

This toolkit is primarily aimed at aiding officers and Information Management Governance Groups (IMGG) with ensuring data protection compliance whenever they handle personal data. It can be used to check general service area compliance, as a reference tool for day to day processes, or engagement in ad hoc or one off projects.

All officers have a duty as outlined in the Data Protection Policy to comply with the Data Protection Act. This toolkit can assist you in complying with the DPA and also allow you to check compliance within your teams.

In addition; all IMGGs have a duty as outlined in their standard Terms of Reference to “Support compliant, effective and secure management and use of information and data across all DU processes and at all stages of the Information Lifecycle: in the collection, use, storage, disposal and archive of information”.

The Information Commissioner’s Office (ICO) is responsible for regulating the Data Protection Act (DPA) and ensuring Data Controllers (such as the London Borough of Barnet) are acting in an appropriate manner when handling personal data.

Following best practice and adhering to this toolkit will assist in mitigating mis-use or loss of personal data and in turn prevent the London Borough of Barnet (LBB) receiving enforcement action from the ICO.

Current supporting Information Management policies can be located on the intranet here.

3. Responsibilities

All individuals and teams handling council data (either working directly for LBB or acting on behalf of LBB) must comply with the Data Protection Act. Breaching the Data
Protection Act could result in disciplinary action. In serious cases breaching the DPA may result in criminal prosecution by the Information Commissioner’s Office.

This toolkit provides guidance and assistance for you to put in place appropriate measures to ensure compliance with the Data Protection Act.

4. **Key definitions**

<table>
<thead>
<tr>
<th><strong>Personal Data</strong></th>
<th>means data which relate to a living individual who can be identified -</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>(a) from those data, or</td>
</tr>
<tr>
<td></td>
<td>(b) from those data and other information which is in the possession of,</td>
</tr>
<tr>
<td></td>
<td>or is likely to come into the possession of, the data controller,</td>
</tr>
<tr>
<td></td>
<td>and includes any expression of opinion about the individual and any</td>
</tr>
<tr>
<td></td>
<td>indication of the intentions of the data controller or any other person</td>
</tr>
<tr>
<td></td>
<td>in respect of the individual.</td>
</tr>
<tr>
<td></td>
<td>N.B. Personal data does not need to be a “name” to allow identification.</td>
</tr>
<tr>
<td></td>
<td>E.g An organisation holds data in an archive unit. The listed records do</td>
</tr>
<tr>
<td></td>
<td>not identify individuals by name, but bear unique reference numbers which</td>
</tr>
<tr>
<td></td>
<td>can be matched to a card index system to identify the individuals concerned.</td>
</tr>
<tr>
<td></td>
<td>The information held is personal data.</td>
</tr>
<tr>
<td><strong>Sensitive personal data</strong></td>
<td>is a subclass of personal data which is given extra protection under the DPA. Sensitive personal data is personal data consisting of information relating to a data subject with regard to: -</td>
</tr>
<tr>
<td></td>
<td>(a) racial or ethnic origin,</td>
</tr>
<tr>
<td></td>
<td>(b) political opinions,</td>
</tr>
<tr>
<td></td>
<td>(c) religious beliefs or other beliefs of a similar nature,</td>
</tr>
<tr>
<td></td>
<td>(d) membership of a trade union (within the meaning of the Trade Union</td>
</tr>
<tr>
<td></td>
<td>and Labour Relations (Consolidation) Act 1992),</td>
</tr>
<tr>
<td></td>
<td>(e) physical or mental health or condition,</td>
</tr>
<tr>
<td></td>
<td>(f) sexual life,</td>
</tr>
<tr>
<td></td>
<td>(g) the commission or alleged commission of any offence, or</td>
</tr>
<tr>
<td></td>
<td>(h) any proceedings for any offence committed or alleged to have been</td>
</tr>
<tr>
<td></td>
<td>committed, the disposal of such proceedings or the sentence of any</td>
</tr>
<tr>
<td></td>
<td>court in such proceedings.</td>
</tr>
<tr>
<td><strong>Data Subject</strong></td>
<td>is an individual who is the subject of personal data.</td>
</tr>
</tbody>
</table>
5. Core guiding principles

There are eight core principles within the DPA. All of the eight principles must be complied with when processing / using personal data in any way. Unless all principles are complied with you will not be fully compliant with the DPA.

5.1. Principle 1 – fairly & lawfully processed

Principle one is arguably the most fundamental of all the principles, and should be the first one you consider and satisfy ahead of processing any personal data. Ensuring the use of personal data is both fair and lawful is crucial to any personal data processing. Fair and Lawful primarily refers to (a) privacy notices and (b) having a clear and justifiable reason for processing the personal data.

Privacy Notices

When collecting personal data not only must you have a legal basis for doing so but you must also be clear and transparent to the data subject as to what your intentions are for the use of the data. To ensure fairness you must provide the data subject with a privacy notice at the point you collect their personal data. A privacy notice can also be known as a fair processing notice.

A privacy notice can be an oral or written statement that data subjects are given when information (personal data) is collected about them, such as via an application form, or via telephone.

The DPA requires that in order for personal data to be processed fairly, the privacy statement must provide the data subject with the following information as a minimum:-

1. the identity of the data controller
2. the identity of any nominated data protection representative, where one has been appointed
3. the purpose(s) for which the data is intended to be processed
4. any further information which is necessary to enable processing in respect of the data subject to be fair e.g. who the data is being shared with

Having a good privacy notice in place can also assist with future information sharing requirements. The council has a standard privacy statement which should be referred to when collecting personal data: -

“Barnet Council has a duty to protect the public funds it administers and may use the information you have provided for the prevention and detection of crime. We may also
share information with other council departments or external organisations in order to undertake our functions as a local authority. We will always comply with the requirements of the Data Protection Act 1998 and never give information about you to anyone else, or use information for another purpose unless the law allows us. If you want to know more about how your information is used visit www.barnet.gov.uk/privacy”

You must use this statement as your privacy notice. If you do not use this statement when collecting personal data you could restrict and limit legitimate use of data sharing.

If you feel that your collection and use of data does not fall within the scope of the council statement and the link provided, or you wish to be more explicit about how the data is going to be used due to the sensitivities of it, you should consult with the Information Management Team before proceeding.

**Lawful**

**Before organisations are able to handle and use personal data they must first identify which schedule of conditions of the DPA they can meet which lawfully allows them to undertake the processing of another person’s data.**

There are a number of conditions that can potentially be used to legitimise the processing of personal data, the most commonly used ones within local government are those of statutory powers or consent.

Remember before you handle / use any personal data you must have identified which Schedule 2 and where necessary Schedule 3 (when processing sensitive personal data) condition(s) you are meeting to allow you to process the information in a legal way.

*See Appendix A for the Schedule 2 and 3 conditions.*

If you are not sure of the conditions which apply please contact the Information Management Team for a clearer interpretation of the conditions and the DPA.

**Consent**

Consent is one of the conditions that can be used to legitimise processing arrangements. This means seeking the consent of the data subject to undertake particular actions in relation to their data.

When relying on consent as justification for processing you should obtain this from the data subjects at the point of data collection.

It is worth considering upcoming changes to the DPA legislation (circa 2017) that will affect consent requirements, and look to future proof your consent. Changes are likely to mean that implied consent will no longer be satisfactory and explicit consent will need to be sought in all cases where consent is relied on. Services and officers will therefore need to provide physical evidence of proof of consent with a signature or voice recording.

It is important to note that consent should only be sought where withdrawal of consent can be actioned. Do not seek consent if there are legitimate reasons to continue
processing the data even when the data subject withdraws consent. There are situations where the council is legally obliged to process data irrespective of consent by a data subject. In these cases, reliance on statutory powers supersedes consent and we should inform the data subject of the processing requirements rather than seek their consent for the processing.

**Withdrawal of Consent or Restricted Processing**

If consent is required for the processing of data, a withdrawal process must also be designed. A clear system must be put in place to ensure withdrawal of consent is flagged and monitored.

Where data is actively shared with other third parties or partner organisations you must ensure any withdrawal of consent is communicated to them.

**ICO Registration**

The London Borough of Barnet is a registered data controller. Our registration document is accessible via the ICO's website. This specifies the registered purposes for which LBB processes personal data.

To see LBB’s registration follow the link below to open the ICO search facility and search for registration Z6665870 which is the council’s registration number.


It is important that the registration is kept up to date and is truly reflective of the council’s processing; as it is a criminal offence not to do so.

**IMPORTANT:** If your team’s processing of personal data is not identified within the currently notification, you need to advise the Information Management Team immediately so that the registration can be updated.

**5.2. Principle 2 – processed for limited purposes**

When collecting personal data you must ensure the data subject is aware of why you are collecting it and what it will be used for. If you later decide you wish to use data you have collected for another purpose, one that was not disclosed to the data subject at the time the data was collected, then the data subject should generally be able to choose whether or not their personal data is used / disclosed in this way, unless one of the DPA exemptions applies.

If you do wish to use or disclose personal data for another purpose that is different from or in addition to the purpose you originally stated you must ensure the new use is fair and lawful, in compliance with principle 1 of the Act.

**5.3. Principle 3 – adequate, relevant and not excessive**

Personal data should only be collected, retained and used where it is necessary and justifiable to do so.
• You should not collect or retain personal data “just in case”. Information should not be retained or collected purely because you think it will be useful in the future.
• Do not email entire spreadsheets when only a column or two of information is required – remove what is not necessary.
• Do not email more people than necessary, only email those with a genuine need to know.
• Consider anonymising information ahead of sending – do you really need to send personal details? Refer to the council’s Anonymisation Policy.

5.4. Principle 4 – accurate and up to date

The responsibility for data quality should be clearly assigned and everyone must understand their individual responsibility in respect of data quality. The Data Quality policy is located on the intranet. When you are notified of any changes/amendments to personal data these must be updated immediately to avoid information becoming inaccurate and out of date. Any other copies of the data must also be updated.

You must:

• take reasonable steps to ensure the accuracy of any personal data you obtain, especially if you are planning to act on it or pass it onto another person;
• ensure that the source of any personal data is clear;
• carefully consider any challenges to the accuracy of information; and
• consider whether it is necessary to update the information.

Where information has been shared with others, you have a responsibility to ensure they are notified of the changes, so their records can also be updated.

5.5. Principle 5 – not kept longer than is necessary

Records retention

LBB has a Records Retention and Disposal Policy published on the intranet which provides guidance on retention periods and examples of the type of records that this includes. This is to support compliance with this principle (5) of the data protection act that states that data should not be kept for longer than is necessary. This policy recommends minimum and permanent retention periods and is reviewed on an annual basis.

Where services have for business reasons adopted a different retention period to the guidelines stated, this should be brought to the attention of the corporate Information Management Team so that the corporate schedule can be updated.

Secure disposal

Shredders are provided at NLBP and confidential waste sacks are also available from facilities for the safe disposal of sensitive or confidential data.
You must never leave a confidential waste sack in the open office overnight. It should either be locked away or you should arrange a collection from facilities and keep control of the sack until it is collected. You should not leave a bag unattended in the expectation that someone is due to collect it.

5.6. Principle 6 – processed in line with Data Subjects rights

Subject Access Request (SAR)

The Data Protection Act provides a right of access to all data subjects to a copy of all personal data a Data Controller holds about them. This is known as the Right of Subject Access and it can be exercised by submitting a written request.

A request of this nature may be difficult to detect as they are sometimes made as part of wider complaint letters. However, the simple rule is if the requester is seeking information about themselves then the request is likely to fall under the SAR provisions and should be responded to accordingly.

Personal information can take a number of forms e.g. paper, electronic, CCTV footage, a picture or even an audio recording. It can include facts and information about a data subject and also include views or opinion of others about the data subject.

In practice, if someone wants to see a small part of their data (a council tax entry or information on their benefits) we need to apply common sense. Such requests should be dealt with quickly and with little formality, although the staff member should still undertake an identity check and should keep a file note of what is provided and when.

All other (non-routine) requests must be directed to your delivery unit Link Officer who has been trained in the requirements of the DPA. They will decide whether to charge the fee, log the request on the Information Management system (iCasework) and advise you what needs to be done.

All staff are responsible for recognising a SAR. For example, requests may be very obvious with the data subject requesting copies of all data relating to them, other times the request may be more subtle and form part of a complaint letter requesting copies of documentation held. On receipt of a SAR the receiving officer must immediately forward the request to their Link Officer.

Subject Access requests have a statutory response deadline of 40 calendar days which must be adhered to and a specific response process should be undertaken.

Any requests of this nature which you are unsure of how to handle should be referred to the Information Management Team as soon as they are received.

SAR Exemptions

There are very limited circumstances where personal data requested by a data subject can be withheld. For example where the information is requested during an on-going criminal investigation and it is not reasonable in the circumstances to disclose.
Please refer to the Subject Access Handling Policy for more information. Any exemptions that are applied must be done so with guidance from your delivery unit Link Officer or a member of the Information Management Team.

You should not apply an exemption without approval of IMT or your Link Officer.

5.7. Principle 7 – keeping information secure

This principle relates to the security and safety of both paper and electronic records.

During the lifecycle of the data, you must ensure it is appropriately protected at all times. Where the data is being managed by another organisation on your behalf, you have a duty and responsibility to ensure you know how the data is being managed and what security has been put in place to protect it.

Data security policies

There is a suite of Information Management Policies in place available on the intranet. Non-compliance with these policies will be dealt with under the relevant council procedures and may result in disciplinary action, termination of contract, or criminal prosecution in the most serious of cases.

The main rule is to be as careful with other people's personal information as we would expect others to be with ours. Good security is good practice and common sense. You should speak to your manager if you have any concerns about information security in your work area.

These Information Management policies are living documents and will be updated at least annually to reflect technological, legal and organisational changes. They should therefore be revisited on a regular basis by all staff. Service heads and service providers are responsible for implementing policies and standards in their area of jurisdiction. Furthermore, these policies and standards must be included in service level agreements and contracts with ICT service providers.

There are some simple steps all staff can take to ensure personal information is kept safe, but further detailed guidance is available in the IT policies contained within the suite of Information Management Policies.

Use of service providers & contractors

When entering into an arrangement with another organisation to handle and process personal data on behalf of the council, you must ensure that the third party meets an appropriate level of security for the type of data they are managing. Sensitive data will require a much higher security threshold.

‘Processing’ is a broad term and covers day to day access to information as well as situations where a contractor has administrative access to a system in order to provide IT support, disaster recovery and similar.
You must not enter into any agreement with a third party which involves the use of personal data unless you have first checked and received appropriate sign off from IS and IMT with regards to the data security requirements in place.

The Due Diligence Security Checklist at Appendix E must be completed and assessed ahead of any arrangement of this nature.

Even where a contract is not required (under the terms of the council’s Contract Procedure Rules) there is still a requirement to have in place appropriate data protection measures.

**NOTE:** A "Data Processor" is someone who is contracted to provide a service on behalf of the council, the data controller (the Council) must, in order to comply with the Data Protection Act (DPA), choose a data processor / service provider who provides sufficient guarantees in respect of technical and organisational security measures which govern how the processing will be done.

A data processor works under the instruction of the council, the council is therefore responsible for the way in which its data processor handles information. If an incident occurs which results in the loss, theft or misuse of data the council may be held responsible if we have not put in place adequate measures and have not undertaken and signed off relevant and appropriate data protection checks.

Remember:

- **Make pre-contractual inquiries with the potential processor**
  
  The council must make inquiries with the potential supplier and should take account of the responses to these inquiries as part of the process when choosing a provider. Copies of letters / documentation should be retained for further reference should an incident occur and they are required by the Information Commissioner.

  Use the Due Diligence Security Checklist at Appendix E. Take account of the responses to these inquiries as part of the process when choosing a provider. Copies of letters / documentation / policies should be retained for further reference should an incident occur and they are required by the Information Commissioner.

  Both physical and electronic measures must be covered, as well as provision for staff training. Copies of appropriate information security policies should be obtained from the contractor/data processor.

  The contract should request the right to make spot checks on the processor’s information security measures and the council must not engage any processor who refuses such access.
ensure adequate contract provisions

A contract or agreement must be put in for all arrangements where third parties are undertaking the processing of personal data for or on behalf of LBB, regardless on the value of the contract.

Standard clauses and further guidance can be sought from the corporate Information Management Team.

make provision for ongoing checks

Regular monitoring of information security policies and compliance must be undertaken. Frequency of checks would be dependent on nature of personal data being processed and circumstances of the contract.

ensure you put in place an exit strategy

Once the arrangement has completed, you need to ensure any personal data which has been handled as part of the contract is appropriately managed. e.g. either returned back to Barnet, securely destroyed or where appropriate agreed to be securely retained by the data processor for an agreed period prior to safe destruction.

5.8. Principle 8 – Personal data not to be transferred to other countries without adequate protection in place

The eighth data protection principle states that personal data must not be transferred to other countries outside the EEA (European Economic Area) without adequate protection.

Data transferred to or hosted outside of the EEA, must only be undertaken with extreme caution following a process of adequacy testing against the security measures in place, this can be a lengthy and time consuming process. Specific approved model contract clauses must be used.

This must be considered especially when using external data storage sites and cloud storage solutions. You must ensure you contact the Information Management Team for further advice and guidance.

6. Project work

The Information Management Impact Assessment (Appendix B) must be completed ahead / during all new projects, changes to data collection methods or new ways of collecting data.

This should be started at the beginning of all projects and forms part of the council’s project toolkit.
Completing this document will allow you to address all the relevant DPA considerations, highlight and raise any concerns well ahead of schedule as well as look at the privacy risks involved in the project.

Any new projects or changes to the way personal data is being processed, shared or stored must be referred to the Information Management Team for input as early on in the project as possible.

Privacy Impact Assessment (PIA)

A Privacy Impact Assessment (PIA) considers the impact a proposed project or policy / policy change will have on the data subjects involved.

It must consider: -

- The privacy of personal data
- The privacy of the individual
- The privacy of personal behaviour
- The privacy of personal communications

The ICO expect this to be completed for all new projects or policies concerning the use of personal data. The first step is to proceed through the PIA screening questions and identify the potential privacy issues.

PIA screening process

<table>
<thead>
<tr>
<th>Question</th>
<th>YES / NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will the project / process involve the collection of new information about individuals?</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Will the project / process compel individuals to provide information about themselves?</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Are you using information about individuals for a purpose it is not currently used for, or in a way it is not currently used?</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Does the project involve you using new technology which might be perceived as being privacy intrusive? E.g. the use of biometrics or facial recognition</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?</td>
<td>YES / NO</td>
</tr>
<tr>
<td>Is the information about individuals of a kind particularly likely to raise privacy concerns or expectations? For example, health records, criminal records or other information that people would consider to be particularly sensitive?</td>
<td>YES / NO</td>
</tr>
</tbody>
</table>
private.

| Will the project require you to contact individuals in ways which they may find intrusive? | YES / NO |

If any of the above questions end up with a “Yes” response you must initiate a full Privacy Impact Assessment.

The ICO Privacy Impact Assessment – Code of Practice provides the relevant templates and further detail on how the process should work.

You can also ask for advice and guidance from the Information Management Team.

7. Information sharing

Information sharing should only be entered into where you have a clear legal basis that allows the sharing to happen. All information sharing arrangements should be discussed with the Information Management Team. Further guidance on the policy surrounding Information Sharing Agreements and Protocols can be found in the Information Sharing Policy.

Within the council

Where a service or team requires information from another service or team, it is the responsibility of both the requesting and the receiving member of staff to ensure they have appropriate authority to request / disclose the information.

With other organisations

The purpose for sharing data with other organisations must be covered by an Information Sharing Agreements, unless it is covered by a one-off exemption. This exemption must however still be documented. Please refer to the Information Sharing Policy for more information.

With key partner organisations

There are many occasions where information will need to be routinely shared between partner organisations and / or third parties. For example, the police, DWP, educational establishments, councillors, or other local authorities.

We must make sure that such sharing arrangements are carried out lawfully and that it is appropriate to share. This means that there must be clear legitimate reasons why the information should be shared, and all eight data protection principles must be adhered to.

All Information Sharing Agreement must be signed off by both the Information Management Team and your service Information Management Governance Group (IMGG) and logged on the corporate information sharing register.
**N.B.** A decision to share personal data with another organisation does not take away your duty to treat data subjects fairly. So before sharing personal data, you should consider carefully what the recipient will do with it, and what the effect on data subjects is likely to be. It is good practice to obtain an assurance about this, for example in the form of a written contract and due diligence checks.

8. **Section 29 - Crime and taxation**

Section 29 of the Data Protection Act 1998, provides an exemption for processing personal data. The exemption can only be used when the request for information is for the purpose of:

(a) the prevention or detection of crime,
(b) the apprehension or prosecution of offenders, or
(c) the assessment or collection of any tax or duty or of any imposition of a similar nature,

Only the police and other organisations that have a crime prevention or law enforcement function, such as benefit fraud departments within local authorities, can use this exemption to help them with their enquiries, by asking the council to disclose personal information about staff or service users.

The exemption is neither a blanket nor automatic exemption and each request should be assessed on a case by case basis.

8.1. **Business as usual requests**

Requests that are considered to be more routine e.g. requests received by Revenue and Benefits s29(3) in relation to taxation fraud queries, should be dealt with by a nominated Revenue and Benefits Officer and processed in line with the Data Protection principles. Consider the following questions ahead of the release of any data and check with IMT if you aren’t sure.

- **Has the request been made in writing?**
- **Are you sure the requester is who they say they are and have a secure email contact address to send the information?**
- **Do you consider the request to be appropriate and proportionate?**
- **Only provide what you consider necessary to meet the objective, and never be worried about challenging a request.**

The service making the disclosure should retain a copy of the request and the reason as to why they either did or didn’t disclose the data. This is to ensure an audit trail exists should a complaint be raised with regards to the disclosure.
8.2. Requests from the police for information

**Council Tax, Benefit or Housing Information**

All s29(2) requests asking for Council Tax, Benefit or Housing information should in the first instance be passed to the CAFT Intelligence Officer email: caft@barnet.gov.uk for handling. This is to ensure a single gateway approach and a consistency with our disclosures. The CAFT Officer will assess the request and process it in line with the Data Protection principles and the guidance provided below.

**All other Information**

All requests concerning the disclosure of other information types should be handled by the relevant service area. If the service area concerned is unclear as to how to deal with the request they should seek assistance from an IMGG representative or a member of the Information Management Team.

A copy of the request and your response should then be sent to the CAFT Intelligence Officer email: caft@barnet.gov.uk for logging. They do not need a full copy of the information provided, but a detailed enough synopsis of what was disclosed or withheld.

The CAFT Officer is responsible for retaining a log of all requests received and dealt with. These are routinely spot checked by the Information Management Team to ensure officers compliance.

8.3. Requests from the police to view files

Requests to view files are more commonly made by the police to social service departments i.e. Family Services and Adults Social Care and Health.

The principles outlined below will apply whether it is a request for information or a request to view a file. You must still undertake the assessment to determine necessity and only provide what is needed and is specific to the investigation the police are undertaking. Be aware of what third party information is held within the file and if necessary remove or redact what you feel is not appropriate to disclose. It is not appropriate to allow the police to look through the whole file because that is easier, or because they are unable to clearly explain what information they need. You would generally only allow full access with the data subject’s consent.

The police should allow you adequate time to compile the relevant file, and allow you to arrange a suitable date and time convenient to you both. Don’t feel pressured into rushing the disclosure; make sure you are happy with it first.

Ensure you make a note on the case file that this access has been provided and on what date.
8.4. General considerations when handling a s29 request

- **Has the request been made in writing?**

  Requests should always be made in writing by letter or email. This means that you can check that the requester has a legitimate business email address or that the request is made on business headed paper. Ensure you obtain a secure email account to send the information to.

- **Why is the person seeking the information? Are they doing it to prevent or detect a crime or apprehend a criminal?**

  The easiest and most appropriate way to gather this information is to ask the requester to complete a suitable *data disclosure form*. Most authorities who request personal information under s.29 will have such forms and will generally use them when making their request.

  If they do not have a suitable *data disclosure form* then ask them to complete the form attached as Appendix C to this guidance note.

- **Consider the possibility of not releasing the information. Will this significantly harm any attempt by the police to prevent the crime, apprehend the criminal etc? Will you be obstructing the investigation?**

  If the requester has not provided reasoning behind the request and merely sought information without explanation, you are within your rights to seek further detail to allow you to make a choice whether to disclose or not.

  Always seek more information from the requester if you aren’t sure what effect your actions not to release will have on the case. This exemption should only be used to release information if its deliberate non-disclosure will hamper the investigation.

- **If you decide to release information, think about what you are releasing. Is the entire request relevant, is the information being sought excessive?**

  Only provide the minimum needed to meet the objective, don’t as a matter of course supply everything. If the objective is unclear seek further information from the requester. Remember, it is down to the requester to provide you with enough information to know that the information being sought is necessary.
How to make the disclosure

Once you have decided you are going to release information, don’t forget to think about how you are going to do this, such as the practical security measures.

Ensure you choose an appropriate method of communication e.g. sending via a secure email connection, or recorded delivery / internal courier for paper records, always ensuring that information is appropriately packaged.

When emailing, check the email address before sending the information. If the information is particularly sensitive, ensure you do a test email first and in all circumstances seek confirmation of receipt from the recipient.

Do I have to disclose the requested information?

This exemption is often misunderstood and misquoted.

It is important to note that s29 is a gateway which allows you to release information. It does not force you to. LBB would still be at fault for disclosing any information the ICO feels is not appropriate regardless of whether this exemption was used. It is therefore important that you assess each request for information correctly.

Section 29 is a discretionary exemption which means the council does not have to comply with the request if it feels that it shouldn’t, for example for confidentiality reasons or it doesn’t feel it has enough information to make an appropriate decision.

You may only feel it is appropriate to disclose part of the request.

If you are in any doubt over why the request is being made and feel you cannot make an appropriate decision, you can go back to the requester and ask them to provide you with a Court Order for the release. A court order will instruct you to release information. On receipt of the court order you can disclose the information as requested on it without fear of breaching the Data Protection Act.

Still not sure?

If you are still not sure or have doubts about the disclosure then contact the Information Management Team for advice.

Remember, it is the council’s decision whether it discloses or not. Whilst the council does of course want to assist the police or any organisation in crime prevention we must be satisfied that the release of data is appropriate. Don’t feel pressured to disclose information, never disclose information over the phone, and always ensure you have sought enough information to allow you to make a clear decision.

9. Section 35 – Legal Advice and Proceedings

This exemption is in the main quoted by solicitors or other local authorities who are defending a case or seeking evidence to support enforcement action.
The s35 exemption states that personal data can only be disclosed to the requester where it is necessary:

- by or under any enactment, by any rule of law or by the order of a court;
- for or in connection with any legal proceedings (including prospective legal proceedings);
- for obtaining legal advice; or
- for establishing, exercising or defending legal rights.

This means that in appropriate circumstances, it would not be unlawful for a data controller to disclose personal data that was needed for legal proceedings or legal advice.

You do not have to disclose personal data in response to a request from a third party simply because this exemption applies. You can choose whether or not to apply the exemption to make a disclosure, and you should do so only if you are satisfied that the disclosure falls within the scope of the exemption. In other words:

- it is necessary for one of the above purposes;
- there is a clear Schedule 2 (and Schedule 3 if applicable) condition that applies; and
- applying the non-disclosure provision would be inconsistent with the disclosure. For example, it would not be necessary for a fair processing notice to have been provided to the relevant data subject regarding such a disclosure.

When faced with a request for disclosure, it can be difficult to decide whether the necessity test can be satisfied. You may also be reluctant to make a disclosure of personal data because of your relationship with the data subject. In such circumstances you may decide not to comply with the request, unless obliged to do so under a court order.

The exemption is not a blanket exemption and each request should be assessed on a case by case basis.

It is important to note that s35 does not force you to disclose information, it merely allows a gateway to do so. LBB would still be at fault for disclosing any information the ICO thought was not appropriate, regardless of whether this exemption was used. It is therefore important that you assess each request for information correctly. If you are unsure you can seek assistance from the Information Management Team.
9.1. **Who processes s35 requests?**

All s35 requests should in the first instance be sent to your service link officer. They will log the request on the icasework system to ensure there is an audit trail and provide advice and guidance as to how the request should be managed.

Guidance can also be obtained from the Information Management Team.

9.2. **General considerations when handling a s35 request**

- **Are you sure the person making the request is who they say they are?**

  Ensure the request is only ever made in writing and ask the requester to complete Appendix D if you have not received sufficient information from their original request. Seek identification if necessary of the requester to assure yourself they are who they say they are.

- **Why is the person seeking the information? Does the request for information fall in to the exemption of requiring information for legal proceedings or legal advice?**

  In order for disclosure to be permitted under this exemption you must be comfortable that the disclosure is necessary for that purpose.

  It is down to the requester to justify the need for the information. Whilst it may prove useful, is it actually necessary? Consider also whether the information is available through other means.

- **Do you owe any level of confidentiality to the data subject?**

  Consider what the data subject was told at the point their information was collected. Was the information obtained in confidence and do we have to uphold that confidence?

- **Is there a “legitimate interest” in disclosing the information?**

  If you feel there is a legitimate interest to the data controller or the requester you must then balance these interests against the interests of the data subject whose data is being disclosed. The “legitimate interests” condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the data subject. Your legitimate interests do not need to be in harmony with those of the data subject for the condition to be met. However, where there is a serious mismatch between competing interests, the data subject’s legitimate interests will come first.
Is the requester fishing for information?

In many circumstances the answer to this question will be “yes”. It is therefore for you to decide whether the information being requested is excessive; can you provide assistance with less information?

When considering what to disclose you may need to break the request down into parts. Remember you do not have to disclose any or all of the information if you do not feel it is appropriate to do so.

How to make a disclosure

Once you have decided you are going to release information, don’t forget to think about how you are going to do this such as the practical security measures.

Ensure you choose an appropriate method of communication e.g. sending via a secure email connection, or recorded delivery / internal courier for paper records, always ensuring that information is appropriately packaged.

When emailing, check the email address before sending the information. If the information is particularly sensitive, ensure you do a test email first and in all circumstances seek confirmation of receipt from the recipient.

The service making the disclosure should retain a copy of the request and the reason as to why they either did or didn’t disclose the data.

A copy of the request and a note stating what information was disclosed should then be sent to the CAFT Intelligence Officer (currently Lucy Connor) for logging. N.B. If the information is particularly sensitive you do not need to actually provide a copy of the request to CAFT, just a note stating what was or wasn’t provided.

Do I have to disclose the requested information?

Each request should be considered on its own merits, and disclosures are made at the discretion of the service Link Officer or corporate Information Management Team.

Remember, s35 is a gateway which allows you to release information. It doesn’t force you to. It is a discretionary exemption which means the council does not have to comply with the request if it feels that it shouldn’t, for example for confidentiality reasons or it doesn’t feel it has enough information to make an appropriate decision.

A common scenario would be a request from a utility company seeking the name and contact details of the council tax payer of a particular address in order to seek the repayment of a debt. With requests such as this we must take into consideration what is “fair” to the data subject. As it is a statutory requirement for people to be registered for council tax it would not be viewed as fair to them for us to then disclose their information to a third party for the purpose of debt collection.

The council may, if it feels it appropriate to do so, disclose information relating to business rates, which would be done so under the provision of the Freedom of Information Act. However, where information requests relate to an individual or a sole
trader, information would not be disclosed unless a court order was issued instructing the disclosure.

Depending on the type of request you receive and the organisation making the request, you may feel it is more appropriate to only disclose part of the information being requested rather than complying with the full request.

If you are in doubt over why the request is being made and feel you cannot make an appropriate decision, you can go back to the requester and ask them to seek a Court Order instructing you to disclose.

On receipt of the court order you can disclose the information as requested on it without fear of breaching the Data Protection Act. Always liaise with legal services first if you are in any doubt, or have any concerns over what the court order is asking you to disclose.

Still not sure?

If you are still not sure or have doubts about the disclosure then contact the corporate Information Management Team for advice.

Remember it is the council’s decision whether it discloses or not. Don’t feel pressured to disclose information, never disclosure information over the phone, and ensure you have sought enough information to allow you to make a clear decision.

10. Data loss / data security incidents

Should an incident occur that has resulted in a loss, suspected loss or misuse or personal data this must be reported immediately to the Information Management Team via data.protection@barnet.gov.uk.

You will need to supply a timeline of events and any initial risk assessment. A full audit trail will need to be maintained throughout the investigation process.

Please refer to the Security and Data Protection Incident Management Policy for further detailed guidance.

11. Communicating with the ICO

The Information Management Team is the corporate lead for any data protection, freedom of information and transparency issues. They are the liaison link between the council and the ICO. All communications to the ICO must be undertaken via IMT to ensure consistency of approach.

12. Data Protection Complaints

Officers who receive any form of complaint relating to a data protection issue, eg. information sharing, access to information, requests to cease processing or any data security concerns must immediately forward a copy of the complaint to data.protection@barnet.gov.uk. The Information Management Team will then advise what steps need to be taken.
APPENDIX A - Schedule 2 & Schedule 3 Conditions

Schedule 2

At least one of the following conditions must be met for personal information to be considered fairly processed:

(a) The data subject has consented to the processing of their information

(b) Processing is necessary for the performance of a contract
   - which the data subject is a party to; or
   - for the taking of steps at the request of the data subject with a view to enter into a contract

(c) Processing is required under a legal obligation (other than one imposed by the contract) which the Data Controller is subject to

(d) Processing is necessary to protect the vital interests of the data subject e.g. an emergency medical situation

(e) Processing is necessary;
   - for the administration of justice
   - for the exercise of any function conferred on any person by or under an enactment
   - for the exercise of any functions of the Crown, a Minister of the Crown or a government department

(f) Processing is necessary in order to pursue the legitimate interests of the Data Controller or third parties (unless it could unjustifiably prejudice the interests of the data subject) to whom the information is being disclosed

This condition must further ensure that once you have established that there is a legitimate interest, these interests must be balanced against the interests of the data subject(s) concerned. The "legitimate interests" condition will not be met if the processing is unwarranted because of its prejudicial effect on the rights and freedoms, or legitimate interests, of the data subject. Your legitimate interests do not need to be in harmony with those of the data subject for the condition to be met. However, where there is a serious mismatch between competing interests, the data subject's legitimate interests will come first.

Finally, the processing of information under the legitimate interests condition must be fair and lawful and must comply with all the data protection principles.

Additional conditions must be met for the processing of sensitive personal information to be "fair".
Schedule 3

When dealing with sensitive personal data an additional condition (known as Schedule 3 condition), must also be met. At least one of the following conditions must be met.

(a) The data subject has given their “explicit” consent to the processing

(b) The processing is necessary to perform any legal right or obligations imposed on the organisation in connection with employment

(c) The processing is necessary to protect the vital interests of the data subject or another person, where consent cannot be given by the data subject, or the organisation cannot be reasonably expected to obtain consent or consent is being unreasonably withheld where it is necessary to protect the vital interests of another

(d) The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject

(e) The processing is necessary in connection with legal proceedings, dealings with legal rights or taking legal advice

(f) The processing is necessary for the administration of justice or carrying out legal or public functions

(g) The processing is necessary for medical purposes
APPENDIX B - Information Management Impact Assessment

This document is an assessment tool that must be completed before all new projects that will be using personal data.

The purpose of this assessment is to identify any risks/issues which will have a detrimental effect on the project, the council or a member of the public through the creation, distribution, archiving or destruction of information assets.

A section on Privacy Impact is included with an assessment tool. Once completed, the assessment should be submitted to the appropriate IMGG (Information Management Governance Group) for sign off or in the absence of this function to the council’s Information Management Team.

### Project Details

<table>
<thead>
<tr>
<th>Project Name</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Project Manager / Point of Contact</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Project Summary</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Brief description of overall activity</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Has anything similar been undertaken before?</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Stakeholders / Organisations involved</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Sponsor</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Activity period</strong></td>
<td></td>
</tr>
</tbody>
</table>
## Information

What type of Information will be collected – be specific (Personal Identifiable Data – data that includes an individual’s name or address, Corporate Sensitive – include corporate budgets etc.)

<table>
<thead>
<tr>
<th>What type of Information will be collected – be specific</th>
<th></th>
</tr>
</thead>
</table>

Why is the information being collected, shared and/or transferred?

<table>
<thead>
<tr>
<th>Why is the information being collected, shared and/or transferred</th>
<th></th>
</tr>
</thead>
</table>

How is the information being collected? (If assets only being shared answer “SHARING” in “Other” and continue “Information Sharing” section)

<table>
<thead>
<tr>
<th>How is the information being collected?</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Verbal ☐</th>
<th>Electronic form ☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Paper questionnaire ☐</td>
<td>Electronic (automated) ☐</td>
</tr>
<tr>
<td>Other →</td>
<td></td>
</tr>
</tbody>
</table>

How is the information being stored?

<table>
<thead>
<tr>
<th>How is the information being stored</th>
<th></th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Paper questionnaire ☐</th>
<th>Electronic form ☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Other →</td>
<td></td>
</tr>
</tbody>
</table>

Where will information will be stored (including backups, copies etc)?

<table>
<thead>
<tr>
<th>Where will information will be stored (including backups, copies etc)</th>
<th></th>
</tr>
</thead>
</table>
How information is to be edited or deleted?

How data is to be quality checked?

Who is responsible for the information?

What are the benefits to the individual and professional?

Sharing and Access

What information is shared?

Who are you sharing it with?

How is the information to be transported/ transferred?
Which roles will have access to the asset? Is there any restrictions based on different roles?

How is it accessed?

How is access to be monitored (audit, logs)?

What security measures will be in place?

What information sharing protocols and operational agreements will be in place?

Has the Due Diligence Security checklist been completed and approved?

Are there plans to store data outside of the EEA? Consider hosted sites, disaster recovery and IT support.
What training is planned to support this piece of work?

Will reports be generated from this information? If Yes will the information be identifiable or anonymous?

Consent

Are individuals being informed of the data collection and the data is being stored / shared at each stage?

How is the individual being informed?

What is the process or obtaining and recording consent (if applicable)?

What is the process if consent is withdrawn to share this information? How is this logged and recorded? (if applicable)
Retention & Disposal

How long information is to be retained?

What is the process for start-up and closing down this piece of work? (Give a brief project plan for aspects regarding information assets).

If the organisation/service ceases, what will happen to the information?

Risks, Issues and Activities

Are there any known information risks or issues at this stage of the project process? Please identify all.

Any known activities that will have a direct effect on this piece of work?

Privacy Impact Assessment

If you answer yes to any of the following questions you must also complete a mandatory Privacy Impact Assessment.

<p>| Will the project / process involve the collection of new information about individuals? | YES / NO |
| Will the project / process compel individuals to provide information | YES / NO |</p>
<table>
<thead>
<tr>
<th>Question</th>
<th>YES / NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will information about individuals be disclosed to organisations or</td>
<td></td>
</tr>
<tr>
<td>people who have not previously had routine access to the information?</td>
<td></td>
</tr>
<tr>
<td>Are you using information about individuals for a purpose it is not</td>
<td></td>
</tr>
<tr>
<td>currently used for, or in a way it is not currently used?</td>
<td></td>
</tr>
<tr>
<td>Does the project involve you using new technology which might be</td>
<td></td>
</tr>
<tr>
<td>perceived as being privacy intrusive? E.g. the use of biometrics or</td>
<td></td>
</tr>
<tr>
<td>facial recognition</td>
<td></td>
</tr>
<tr>
<td>Will the project result in you making decisions or taking action against</td>
<td></td>
</tr>
<tr>
<td>individuals in ways which can have a significant impact on them?</td>
<td></td>
</tr>
<tr>
<td>Is the information about individuals of a kind particularly likely to</td>
<td></td>
</tr>
<tr>
<td>raise privacy concerns or expectations? For example, health records,</td>
<td></td>
</tr>
<tr>
<td>criminal records or other information that people would consider to be</td>
<td></td>
</tr>
<tr>
<td>particularly private.</td>
<td></td>
</tr>
<tr>
<td>Will the project require you to contact individuals in ways which they</td>
<td></td>
</tr>
<tr>
<td>may find intrusive?</td>
<td></td>
</tr>
</tbody>
</table>
APPENDIX C – Section 29 Requester Template

Request for Disclosure of Personal Data under s29 of the Data Protection Act 1998

Section 1 - Requester details:

| Requester Name: | ______________________________________________ |
| Organisation Name & Address: | ______________________________________________ |
| Requester Job Title: | ______________________________________________ |
| Telephone Number: | ______________________________________________ |
| Secure email address: | ______________________________________________ |

Section 2 – Data Subjects Details:

Information being requested:
(please provide details of what information is being sought. Feel free to attach additional documentation where necessary)

Section 3: Justification for disclosure

Type of offence:

Reason why the information is necessary:

State which statutory power you are requesting the information under:
Section 4: Authorisation
I confirm that the data being requested is required for one of the following purposes, and non-disclosure will prejudice that purpose: -

- [ ] the prevention or detection of crime,
- [ ] the apprehension or prosecution of offenders, or
- [ ] the assessment or collection of any tax or duty or of any imposition of a similar nature,

I further confirm that any information disclosed to me will not be used in any way which is incompatible with this purpose.

<table>
<thead>
<tr>
<th>Signed:</th>
<th>Dated:</th>
</tr>
</thead>
<tbody>
<tr>
<td>________________________________</td>
<td>(requesting officer)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signed:</th>
<th>Dated:</th>
</tr>
</thead>
<tbody>
<tr>
<td>________________________________</td>
<td>(authorising officer)</td>
</tr>
<tr>
<td>Print Name:</td>
<td>________________________________</td>
</tr>
<tr>
<td>Job Title:</td>
<td>________________________________</td>
</tr>
</tbody>
</table>
APPENDIX D – Section 35 Requester Template

Request for Disclosure of Personal Data under s35 of the Data Protection Act 1998

Section 1 - Requester details:

Requester Name: ________________________________________________

Organisation Name & Address: (if applicable) _________________________

Telephone Number: ______________________________________________

Email address: __________________________________________________

Please mark as appropriate:
➢ I am a private individual acting on my own behalf ☐
➢ I represent a client(s) ☐
➢ Other (please state) ☐

Section 2 – Data Subjects Details:

Name of the person you are seeking information about:
___________________________________________________________________

Information being requested:
(please provide exact details of what information is being sought. Feel free to attach additional documentation where necessary)

Section 3: Justification for disclosure

Please mark as appropriate your reason for application:
➢ in existing legal proceedings (s35(2) DPA) ☐
➢ in prospective legal proceedings (s35(2) DPA) ☐
➢ to obtain legal advice (s35(2) DPA) ☐
➢ to establish, exercise or defend a legal right (s35(2) DPA)* ☐

* Please describe the legal rights that you are intending to establish, exercise or defend.
The purpose and **necessity** to provide this information to you is key to determining a lawful disclosure within the provisions of the Data Protection Act 1998. You should only request information which is **necessary** in your case.

Reason why the information is necessary:

---

**Section 4: Authorisation**

I confirm that the information requested is necessary for the purposes described in this application and that failure to provide the data will, in my view, is likely to prejudice these matters.

I further confirm that any information disclosed to me will not be used in any way which is incompatible with this purpose.

| Signed: | Dated: |
APPENDIX E1 - Due Diligence Security Checklist Template

As part of regular auditing, service providers are required to produce confirmation of relevant policy, procedures and documentation, to ensure the security and safety of our information.

These will be evaluated in line with Barnet Council’s standards and expectations. If the policies and procedures are deemed unsatisfactory, the application is unlikely to be progressed.

Please ensure you provide enough information to assist us in determining satisfactory reassurance with regards to the protection of information.

<table>
<thead>
<tr>
<th>Documentation</th>
<th>Provided?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information governance, security and sharing policies</td>
<td></td>
</tr>
<tr>
<td>Please provide a copy of any relevant policies and procedures which can be referred to for review.</td>
<td></td>
</tr>
</tbody>
</table>

Any supporting comments/notes:

Please answer the following questions. These will be reviewed (along with the Information governance, security and sharing policies provided) to ensure that council is satisfied that the provider has adequate security measures in place to protect the council’s data. The provider is expected to have processes which ensure that personal data is processed and stored securely and the that measures are either in place or will be taken to prevent unauthorised access.

<table>
<thead>
<tr>
<th>Do you have a valid and up to date notification with the Information Commissioner Office (ICO) to cover all your personal data processing arrangements? Please provide your registration number.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes [ ] No [ ]</td>
</tr>
<tr>
<td>Registration number: _______________________________________________________________</td>
</tr>
</tbody>
</table>

38
Who within your organisation is responsible for compliance with the requirements of the Data Protection Act? Please provide details of their role.

Please provide details of Data Protection training undertaken by your organisation and staff.

How do you take reasonable steps at the recruitment stage to check the identity and reliability of your staff? For example, by getting references and checking that these and the person's qualifications are valid.

If your service allows for you to host systems/store data on behalf of the council can you confirm what country the data/systems are located in? Can you also confirm whether this location will remain the same during possible server outages/system failures or will the system automatically switch to another server located in an alternative location?
Please provide details of any data security or data protection incidents either reported to the ICO or handled within your organisation over the past 2 years.

N.B. We may seek further information or clarification on receipt of this information.

NOTE TO BARNET COUNCIL OFFICERS:

If you are unclear as to whether the above responses provide an appropriate level of security for the procurement you are entering into, please contact the Barnet Information Management Team via email at data.protection@barnet.gov.uk for further advice.
APPENDIX E2 - Due Diligence – Evaluation Guidance

On receipt of the due diligence checklist above, below are some of the factors that the supplier’s response should address:

- How well do they protect unauthorised access e.g. firewalls, virus checking is in place?
- How often does the organisation carry out updates to installed software including installation of patches?
- Which staff have access to the information? Are there restrictions in place?
- How often passwords are required to be changed?
- Is paper waste dealt with securely?
- How often are staff trained?
- How do they manage physical security of data?
- Can fax messages be sent and received securely?
- How often is information backed up and how is it securely stored?
- Is the provider using cloud storage, has the storage solution been assessed and approved for use by Barnet?
- Do they process or access information outside of the European Economic Area?

On receipt of policies, these must be reviewed to ensure they cover the appropriate areas of concern.

The council must be satisfied that the supplier has adequate security measures in place to protect the council’s data.

To decide what measures are appropriate you need to take into account the sort of information you have, the harm that might result from its misuse, the technology that is available to protect the information and also what it would cost to ensure an appropriate level of security.
13. Review of the Policy

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

14. Contact Information/Further Guidance

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

Tel: 020 8359 2029

Email: data.protection@barnet.gov.uk

Policy Pages: Information Management Policies