MEETING **GENERAL FUNCTIONS COMMITTEE**
DATE AND TIME **TUESDAY 25TH MARCH, 2014** **AT 7.00 PM**
VENUE **HENDON TOWN HALL, THE BURROUGHS, NW4 4BG**

Dear Councillors,

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

Item No	Title of Report	Pages
9.	Information Management Policies	1 - 48

Maria Lugangira 020 8359 2761
maria.lugangira@barnet.gov.uk

This page is intentionally left blank

AGENDA ITEM 9

Meeting	General Functions Committee
Date	25 March 2014
Subject	**Information Management Policies**
Report of	Deputy Chief Operating Officer
Summary of Report	This report seeks the approval of the committee of new and revised Information Management policies that apply to Members.

Officer Contributors	Victoria Blyth, Information Manager Jenny Obee, Head of Information Management
Status (public or exempt)	Public
Wards Affected	Not Applicable
Key Decision	Not Applicable
Reason for urgency / exemption from call-in	N/A
Function of	Council
Enclosures	**New Policy** Appx 1 - Members Access to Information Policy v1.0 Appx 2 - GCSx Protective Marking for Emails Policy v1.0 **Revised Policies** Appx 3 - Acceptable Use Policy v8.0 Appx 4 - BlackBerry Policy v1.0 Appx 5 - PSN Acceptable Use Statement
Contact for Further Information:	Jenny Obee, Head of Information Management jenny.obee@barnet.gov.uk

1. RECOMMENDATION

1.1 That the committee approves the new policies on Members Information Management and GCSx Protective Marking for Emails, and the revised policies on Acceptable Use and BlackBerrys.

1.2 That the Information Security Manager be instructed to ensure that all Members with a GCSx email account have signed a copy of the PSN Acceptable Use Statement

1.3 That the Head of Information Management in conjunction with the Head of Information Systems be instructed to publicise the policies to Barnet systems and equipment users.

2. RELEVANT PREVIOUS DECISIONS

2.1 General Functions Committee, 14 January 2009, Decision item 17, Information Systems Policies.

3. CORPORATE PRIORITIES AND POLICY CONSIDERATIONS

3.1 The Council's corporate plan for 2013-15 sets our strategic priorities as:

- "promote responsible growth, development and success across the borough;
- support families and individuals that need it – promoting independence, learning and well-being; and
- improve the satisfaction of residents and businesses with the London Borough of Barnet as a place to live, work and study".

3.2 The introduction and revision of these policies underpins the appropriate use, storage and security of information, ensuring that information is available when required by Members to make robust, evidence based decisions to support realisation of these strategic priorities. As information is a strategic asset for Barnet, it is important that it is managed well – managing information 'well' includes ensuring that it is stored and used safely and in accordance with information legislation. These policies set out the requirements of Members in ensuring that information is managed accordingly.

4. RISK MANAGEMENT ISSUES

4.1 The absence of effective corporate policies leaves the Council exposed to risk if sensitive or confidential information is lost. This loss can be through human error, but also through unauthorised use of Council equipment. It is therefore important that we put into place appropriate risk mitigations against information loss – this includes technical controls such as effective anti-hacking measures and password protection of equipment, as well as implementing policy to ensure that staff and Members are aware of the requirements for operating safely and securely.

4.2 The Council is connected to the Public Services Network (PSN), a Government network which provides connections between public sector organisations such as Central Government Departments and Local Authorities. Connecting to the PSN allows the Council to access several key central government services, including the GCSx system for communicating securely and the DWP system that enables us to run the Revenue and Benefits service in the borough. Barnet's use of the PSN requires us to meet the controls set out in the PSN Code of Connection, which we must meet annually to retain our PSN connection. The implementation of effective policy is a necessary control within the PSN Code of Connection.

5. EQUALITIES AND DIVERSITY ISSUES

5.1 These policies help to ensure the security of information and technology and have no effect on staff or Members in terms of race, ethnicity, sexual orientation, age of religion.

6. USE OF RESOURCES IMPLICATIONS (Finance, Procurement, Performance & Value for Money, Staffing, IT, Property, Sustainability)

6.1 The specific costs of introducing and maintaining these policies are minimal and met within current budgets. Supporting these policies technically is included within the business as usual activities of the Information Systems Team.

7. LEGAL ISSUES

7.1 The council and its elected Members are obliged to abide by information management legislation including the Data Protection Act 1998, the Freedom of Information Act 2000, the Environmental Information Regulations 2004. In addition Members have individual responsibility for complying with the Data Protection Act 1998.

7.2 The council accesses the Public Services Network (PSN), which allows the council secure contact with government agencies such as the Department for Work and Pensions (DWP). The PSN requires the council to meet their requirements in areas such as information security in order to remain on the network. These policies cover some of the requirements relating to network users.

8. CONSTITUTIONAL POWERS (Relevant section from the Constitution, Key/Non-Key Decision)

8.1 Council Constitution, Responsibility for Functions, Terms of Reference of General Functions Committee, All other Council Functions that are not reserved to the Council.

9. BACKGROUND INFORMATION

9.1 The council will be taking part in an audit by the Information Commissioner's Office (ICO) into the council's data protection practices in July 2014. The council therefore wishes to ensure that information legislation policies reflect current working practices and incorporate the most recent ICO and industry guidance.

9.2 The council and its elected Members are obliged to abide by information management legislation including the Data Protection Act 1998, the Freedom of Information Act 2000 and the Environmental Information Regulations 2004. In addition, Members have individual responsibility for complying with the Data Protection Act 1998. Guidance has been requested by Members on what their responsibilities are under relevant information legislation, both as representatives of the council and as elected ward representatives. In addition, guidance has been requested by officers to clarify their obligations to provide Members with access to information.

9.3 The new Members Information Management Policy clarifies rights of access to information. Bringing the information legislation that applies to Members into one policy means that Members do not have to read and comply with council-wide information legislation policies such as the Data Protection Policy, as these are in-depth operational requirements that are more detailed than are required by Members. The new policy brings current working practices together into one policy.

9.4 The council accesses the Public Services Network (PSN), which allows the council secure contact with government agencies such as the Department for Work and Pensions (DWP). Access to the PSN is critical for, for example, provision of a revenues and benefits service.

9.5 The PSN authority requires the council to meet a stringent set of requirements in areas such as information security in order to remain on the network. These policies cover some of the requirements relating to network users.

9.6 Policy Summary

- Members Information Management Policy – This policy clarifies a Member's rights of access to information and their responsibilities under information legislation, both when acting as a Member of the Council and handling council information, and also when acting as a ward representative where they are solely responsible for the handling of information.
- GCSx Protective Marking for Emails Policy – GCSx is a secure email service used by the council for the secure transmission of electronic information. It is heavily used in Adults and Children's Services and by some Members for their committee work. GCSx forms part of the PSN network and as such the council is obliged to abide by stringent requirements, which include ensuring that users are individually aware of their responsibilities.
- Acceptable Use Policy - This policy sets out the manner in which the council's computer systems are utilised and is designed to protect the confidentiality, integrity and availability of its information systems. The policy provides an insight into what Barnet requires from its equipment and system users in order to reduce risks to the network and the risk of data getting into the wrong hands through the misuse of corporate infrastructure.
- BlackBerry Policy – This policy confirms the requirements of all BlackBerry users and helps to ensure that the council protects its entire network as well as personal and confidential information while using mobile smart phone devices.

- PSN Acceptable Use Statement – The council's use of the PSN places stringent obligations on the council, which include ensuring that network users abide by those requirements. The council needs to keep a record that every GCSx account user has read and agrees to abide by these requirements by signing the statement.

10. LIST OF BACKGROUND PAPERS

10.1 None

Cleared by Finance (Officer's initials)	**AD / JH**
Cleared by Legal (Officer's initials)	**CE**

This page is intentionally left blank

Members Information Management Policy

London Borough of Barnet

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). Request can be made for information held by the council, which includes Members acting in their role as 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.

The council's Access to Information Procedure Rules, part of the council's Constitution, provide Members with details of their rights to inspect council documents. These rules relate specifically to information concerning meetings of the Council and covers rights established under the Local Government Act 1972 (as amended), among others.

Beyond these, a Member has a right to request information where they can show a 'need to know' that information in order to perform their duties as a councillor. This is particularly relevant where a Member is requesting personal information about an individual. Access to information under this common law right necessitates a

Member demonstrating their ‘need to know’, and this requirement has been covered in case law. Guidance on use of information is in section 8 of this policy.

In many circumstances a Member’s ‘need to know’ will normally be presumed, such as a committee member wishing to inspect documents or briefings relating to the functions of that committee. However, the law does not allow a ‘roving commission’ and in some circumstances, such as when requesting personal information about individuals, the motive for requesting information will be relevant and a Member will be expected to justify their request for information. The determination of the need to know will initially be carried out by the relevant service, who may seek advice from the Information Management Team.

7.2. Local Authority Accounts

The Audit Commission Act 1998 and the Accounts and Audit (England) Regulations 2011 provide a right to inspect the council’s accounts and question the auditor, although the rights are restricted to prevent access to personal information.

Requests to access information under these rights should be made to the council’s Deputy Chief Operating Officer.

7.3. Member Enquiry Service

The Member Enquiry Service is the way of requesting information from officers. 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 10 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.

It is therefore likely that Members will receive more information if they ask the council directly via the Members Enquiry service.

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.

Disclosing confidential information may be considered a breach of the Members Code of Conduct.

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.

8.2. Data Protection

Personal information held by Members on behalf of the council must be handled appropriately and kept secure. Section 9 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.

8.3. Passing on Information from Constituents

Where a constituent has contacted a Member directly, they are usually doing so in a Member's capacity as their elected 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 as defined by the DPA, such as medical details, is concerned. The ICO's Good Practice Note provides more information on a Member's responsibilities.

9. Handling of Information

9.1. 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.

9.2 Access to council systems and information

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

Giving access to this equipment to anyone except the council IS department is not allowed. In normal circumstances users should not attempt to access the council's network from privately owned devices, unless this has been agreed with IS, as this puts the council's network at risk.

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 IS if this is appropriate, as it may put council information and the council network at risk. Some countries are banned from connecting to Public Services Network connected networks. Certain countries may confiscate encrypted devices on entry and/or force a user to enter passwords and bypass security. Confiscated devices may not be returned.
Please contact the IT service desk itservicedesk@barnet.gov.uk 020 8359 3333 to have roaming enabled on your device.

9.3 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.
- Don’t keep papers records with valuables when in the home or workplace as these are often the primary target for thieves.
- 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.

9.4 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 9.3 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.

9.5 Loss of equipment or information

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

- IT servicedesk on 020 8359 3333
- Insurance team on 020 8359 7197
- Information Management Team data.protection@barnet.gov.uk or 020 8359 2029.

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.

10 Records Retention

10.1 General Principles

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

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

It is not allowable to keep personal information 'just in case' nor to use it for a different purpose than it was originally given. The ICO has detailed guidance.

10.2 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.

10.3 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 10.1, personal information should only be kept as long as necessary, only used for the purpose it was originally given, and disposed of securely.

10.4 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.

11 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 10 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

12 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 Flr, 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

Putting the Community First

BARNET
LONDON BOROUGH

Protective Marking for GCSx Emails Policy

How to protectively mark GCSx emails

Contents

1. What is information security?

The council has a responsibility to balance openness with security and aims to ensure that information is appropriately protected from loss, unauthorised access and disclosure. Information Security is the preservation of the confidentiality, integrity and availability of information.

Confidentiality ensures that information is accessible only to those authorised to have access.

Integrity safeguards the accuracy and completeness of information and processing methods.

Availability ensures that users have access to information and associated assets when required.

2. What is protective marking?

Protective marking is a way of ensuring that access to information and other assets is correctly managed and that assets are safeguarded to an agreed and proportionate level throughout their lifecycle. It is also a way of indicating to others the levels of protection required to prevent the compromise of the information.

The protective marking you apply to information must accurately reflect the sensitivity and value of the information.

Applying too high a protective marking can affect the *availability* of information by inhibiting access, leading to unnecessary and expensive protective controls, and impairing the efficiency of the council's business.

Applying too low a protective marking may lead to damaging consequences and compromise of the *confidentiality* and *integrity* of the information.

The Government Protective Marking System (GPMS) currently has 6 levels of protective marking:

- **TOP SECRET**
- **SECRET**
- **CONFIDENTIAL**
- **RESTRICTED**
- **PROTECT**
- **UNCLASSIFIED**

UNCLASSIFIED and PROTECT are relevant to Barnet Council when looking at marking GCSx emails. The definitions can be seen in the table at Appendix A.

It is rare that something you need to email would be considered RESTRICTED. The GCSx network is not designed to carry RESTRICTED information. If you feel that you have RESTRICTED information please contact the Information Management Team to discuss alternative ways of sending this. In order to be classified as RESTRICTED information would need to be likely to for example: cause prolonged and significant distress for an individual, cause serious injury, cause public sector loss in excess of £1M, affect authority wide disruption that could pose a health risk.

CONFIDENTIAL is a national security classification used by the government that requires a higher level of security than would be appropriate for any council information; compromise of which would have national security or national economic ramifications. No information handled by you day-to-day will merit a protective marking of CONFIDENTIAL.

2.1. Unclassified marking for GCSx

You are required to use protective marking on every email sent via the GCSx connection. As GCSx is a system designed specifically for the sending of information via a more secure route, you would not normally think it appropriate to mark a GCSx email as UNCLASSIFIED or NOT PROTECTIVELY MARKED. However, as some organisations only have GCSx as their default method of communication you may have no option but to use GCSx regardless of the sensitivity of the message. Thereby resulting in you sending information via GCSx that does not need a higher level of security and could be marked UNCLASSIFIED.

3. What is sensitivity marking (descriptors)?

As the council deals with a large range of information that can be classified by PROTECT you can add a sensitivity marking after the protective marking to allow you to better describe why the information is protected.

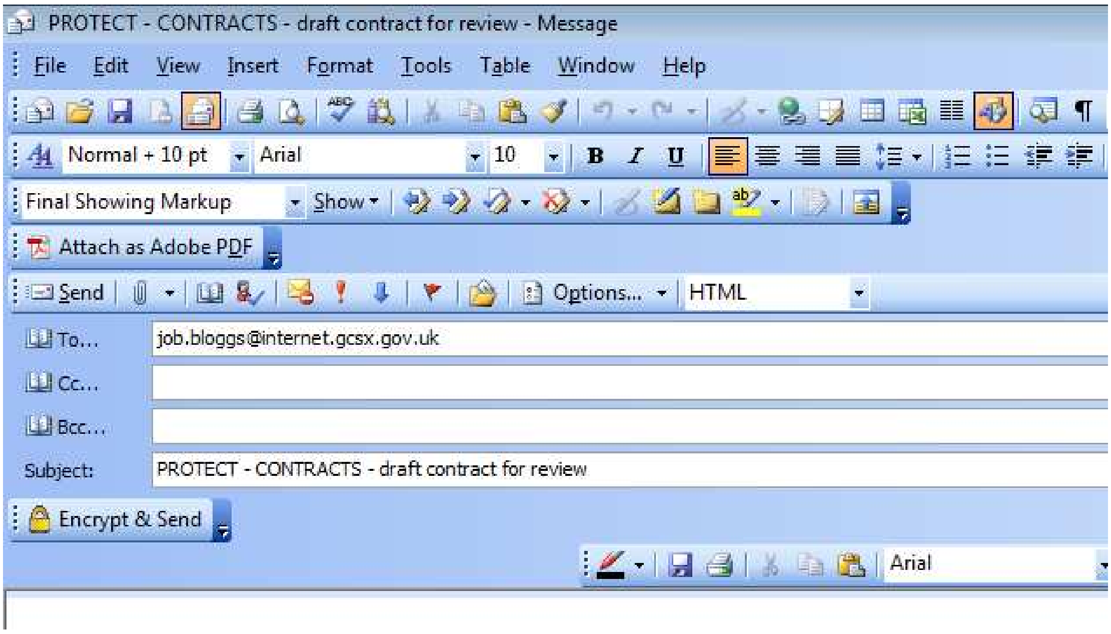
For example “PROTECT – INVESTIGATIONS” or “PROTECT – CONTRACTS”

Also known as ‘caveats' or ‘descriptors', sensitivity markings can provide extra information to enable the ‘need to know' principle to be applied effectively. See the table at Appendix B for a list of descriptors for Barnet Council information.

The list is not exhaustive so you can create new ones that are relevant to your area of work. However, you need to inform Information Management if you do so, to enable us to keep track of what descriptors are being used by services.

4. What you need to do

If you are sending an email using your GCSx account you must use the subject line to classify the email using protective marking. This should look like the image below with the protective marking, descriptor (if appropriate) and then subject title.



PROTECT - CONTRACTS - draft contract for review - Message

Normal + 10 pt | Arial | 10

HTML

To... job.bloggs@internet.gcsx.gov.uk

Cc...

Bcc...

Subject: PROTECT - CONTRACTS - draft contract for review

Arial

It is the responsibility of the sender to protectively mark the email. If you are including attachments you may need to check with the document author what level of protection is appropriate and therefore what level of protective marking the email requires. Similarly, if you are sending an email on behalf of a colleague or senior manager you may wish to check what level of marking is required if it is unclear.

5. Material originating outside of the council

There is no agreed UK system for marking sensitive material, although terms such as **private** and **confidential** are in common use, particularly in relation to personal information. Any material originating outside of the council, that is not covered by a recognisable protective marking, international agreement, contract or other arrangements, but is marked in such a way to indicate sensitivity, must when handled by the council, be protected to at least the level offered by the PROTECT marking, and a higher marking may be considered.

6. Information Rights

The protective markings do not impose any classification to restrict or to supply information under the Freedom of Information Act, Data Protection Act or Environmental Information Regulations. However, they may indicate that all or some of the information may be subject to exemptions, for example personal information. A protectively marked email is not automatically exempt from any information rights legislation.

It is worth noting that any information which has been (or would be) released in response to a FOI request would normally be considered as UNCLASSIFIED.

7. APPENDIX A - Protective Marking Categories

Protective Marking Categories for GCSx emails

Impact that *would be likely* if the data is disclosed, lost or stolen and misused	**Protective Marking**	**Examples**	**Impact Level**
Little or no impact on the finances of the council Little or no inconvenience or distress to the customer Little or no financial impact to the customer Little or no impact on the council's standing or reputation.	**NOT PROTECTIVELY MARKED / UNCLASSIFIED**	Policies and procedures Documents available in the public domain or on the council's website Property address where it does not identify the individual owner or residents (a full postcode can sometimes be considered to identify an individual) Names and contact details of specific employees or individuals that are in the public domain or where an individual has authorised this	0 or 1
Short-term inconvenience, harm or distress or significant embarrassment to an individual Cause financial loss or loss of earning potential, or to facilitate improper gain Damage to the council's standing or reputation Financial impact to the council (up to £1M) Breach proper undertakings to maintain the confidence of information provided by individuals or third parties Breach statutory restrictions on the disclosure of information	**PROTECT**	Personal information relating to any customer or employee such as a name, address and contact details, bank details, VAT number or National Insurance number, for which we have a duty of care Exempt Committee papers excluded from the public under Local Government Act An employee record including a disciplinary or grievance file A customer case file Draft documents before approval for release into public domain	2

Unclassified marking for GCSx

The term “UNCLASSIFIED“ or “NOT PROTECTIVELY MARKED“ may be used to indicate positively that a protective marking is not needed.

You are required to use protective marking on every email sent via the GCSx connection. As GCSx is a system designed specifically for the sending of information via a more secure route, you would not normally think it appropriate to mark a GCSx email as UNCLASSIFIED or NOT PROTECTIVELY MARKED. However, as some organisations only have GCSx as their default method of communication you may have no option but to use GCSx regardless of the sensitivity of the message. Thereby resulting in you sending information via GCSx that does not need a higher level of security and could be marked UNCLASSIFIED.

Under no circumstances should UNCLASSIFIED be used where a decision has not yet been made on the classification of a document or email.

RESTRICTED classification

It is rare that something you need to email would be considered RESTRICTED. The GCSx network (and the Encrypt and Send application) is not designed to carry RESTRICTED information. If you feel that you have RESTRICTED information please contact the Information Management Team to discuss alternative ways of sending this.

In order to be classified as RESTRICTED information would need to be likely to for example: cause prolonged and significant distress for an individual, cause serious injury, cause public sector loss in excess of £1M, affect authority wide disruption that could pose a health risk.

8. APPENDIX B - Descriptors for Protective Marking

The table below defines how a descriptor may be used with the PROTECT marking based on information content. For example, PROTECT – CONTRACTS. They are not mandatory and they do not mean that, for example, every contract must be considered to have the PROTECT classification.

The descriptors serve to help those handling the information to decide which people should have access to the material. Information received from public sector partners may use one of these descriptors so you may receive information marked in this way. The list is not exhaustive so you can create new ones that are relevant to your area of work. However, you need to inform Information Management if you do so, to enable us to keep track of what descriptors are being used by services.

Descriptor	
COMMERCIAL	Disclosure would be likely to damage a third party or commercial establishment's processes or affairs
CONTRACTS	Tenders in progress and contract terms accepted
INTERNAL	Only available to LBB employees and should not be published or circulated outside of LBB without permission
INVESTIGATIONS	Investigations into disciplinary affairs or may lead to criminal cases
LEGAL PROFESSIONAL PRIVILEGE	Contains legal opinion that would be considered exempt under the Freedom of Information Act or could harm the council's interests if disclosed
MANAGEMENT	Policy and planning affecting the interests of the Authority or staff
MEDICAL	Medical reports, records and material relating to an individual
PERSONAL	Information that is personal to an individual or the sender and/or recipient
POLICY	A report or policy document that is for debate and consideration (policies once agreed would normally be publicly available)
STAFF	Contains references to named or identifiable staff or personal confidences

Acceptable Use Policy

London Borough of Barnet

Contents

1. Introduction

The purpose of this policy is to:

- protect the information assets owned and used by the council;
- protect other services or networks to which the council is connected from misuse;
- ensure compliance with all regulatory, legislative and internal policy requirements.

This policy applies to users of computer services and equipment that are provided by London Borough of Barnet (LBB), or its ICT providers; including Members, employees, temporary staff, contractors, partners and any authorised 3rd parties. It does not apply to council services provided to the public. It also applies to the use of services on all council devices including mobile equipment such as BlackBerrys or mobile phones and tablets or laptops. Please note this policy applies:

- whether you are using the equipment at work or off council property.
- when using the equipment with any internet connection whether work, personal or public.

Any actual or suspected breaches of this policy will be thoroughly investigated, and in the event of staff or Member misconduct will be dealt with under the council's disciplinary procedure or the Member's Code of Conduct complaints procedure respectively. Any suspected breaches that may constitute a criminal offence will also be reported to the council's Corporate Anti Fraud Team (CAFT) for investigation.

Staff are responsible for identifying to their line manager any concerns with work processes or other local arrangements that prevent them from complying with this policy. Line managers are responsible for ensuring that staff are supported in complying with this policy. Members should seek advice from the Council's Chief Finance Officer or Monitoring Officer when using resources of the Council if there are concerns regarding complying with this policy.

Access to council information systems and equipment is provided by the council for Members to use in their three roles of Member of the Council, ward representative and political party/independent member. The equipment belongs to the council throughout its useful life. At the end of its useful life the council may consider options for Members purchasing the equipment, however this should not be assumed.

It is recognised that Members will use equipment and systems outside of traditional working hours and mainly from private or public internet connections. However, the principles in this policy apply to all Members as they do to staff, with the exception that Members can use council email for communication of political beliefs.

Suspected breaches of this policy by Members may warrant investigation and in any event will be reported to the Leader of the Council, Leader of the relevant Party Group, Chief Executive and/ or Monitoring Officer. Any suspected breaches that may constitute a criminal offence will also be reported to the council's Corporate Anti-Fraud Team (CAFT) for investigation.

2. General Computer Use

2.1 Passwords

Access to Council systems and data is through user identification and passwords. Mobile phone must be protected with a PIN number; BlackBerrys with a 'strong' password as described in the BlackBerry User Policy. The characteristics of a 'strong' password include the following:

- At least 8 characters long
- A mix of alphabetic, numeric and special characters
- Not based on a pattern e.g. 12345678

Further information is included within the Password Policy.

2.2 Personal use

Access to council information systems and equipment is provided to assist users in the performance of their jobs. Where access and equipment is provided its use should be limited to official council business. However, it is recognised that there may be occasions outside of work time or during lunch breaks when users wish to use them for personal reasons. Reasonable personal use of council internet and email services is permitted provided it complies with this policy and any policies and legislation referred to in this policy.

Examples of unreasonable personal use are:

- The use of council Information Communication Technology (ICT) services to operate any business or for work outside of council employment.
- When the personal use of internet facilities affects a user's work performance.
- Time wasting and large amounts of continuous usage.
- Wasteful use of resources.

- Saving of non-council data on the council network (including ‘home drives’). These can and will be deleted to minimise expenditure on storage and back-ups.
- The printing of large documents.
- Sending or receiving large documents or large numbers of emails.
- Access to websites prohibited under council policies (including material considered offensive in any way such as sexually explicit, discriminatory, defamatory or libellous material).
- The use of systems or the internet for personal gain, examples include gambling and trading. No personal websites may be hosted on council equipment.
- Use of the system should not have a noticeable effect on the availability of the system for others. Therefore users should not participate in resource intensive online games or have active any web channels that broadcast frequent updates to your computer.

Under no circumstances should users allow others such as family or friends to use systems or equipment provided by the council.

All users of council systems are responsible for the professional, ethical and lawful use of those systems. Access is granted on the basis that the user understands and adheres to this policy and agrees that system usage, including personal use, will be subject to monitoring by the council for policy compliance.

2.3 Hardware use

All ICT equipment provided to users including Members, employees, temporary staff, contractors, partners and any authorised 3rd parties remains the property of the council. It is to be returned to LBB if it becomes defective or when no longer required for the role in which it was issued, for example, at the end of term in elected office, end of employment or end of contract.

No council data should be copied to removable media without express authorisation.

No peripheral devices of any kind (cameras, PDAs, mobile phones, unencrypted USB drives etc) may be installed or configured on, or connected to any council computer unless authorised and installed by Information Services (IS). If you have a requirement to use the CD drive or USB ports on any equipment you will need to raise a policy exception request by contacting the IT service desk.

2.4 Remote working

Only 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 wifi via Citrix or VPN, or through Mobile Iron technology on tablet devices.

More detailed information (for staff) is included in the Remote Working Policy.

2.5 Use of personal equipment or email accounts

On a day to day basis the use of personally owned equipment or personal email accounts for council business is forbidden. If working from home is required on either a regular or ad hoc basis this should only be conducted on council or authorised 3rd party equipment.

However, during business continuity incidents such as building failures or extreme weather it is accepted that some council business could be conducted on personal equipment when agreed by your line manager. Personal information must only be dealt with when absolutely necessary and not for the sake of convenience. Sensitive personal data (as defined by the Data Protection Act 1998, such as medical or equalities information) should never be sent to or processed using non-council provided equipment.

Any use of personal email accounts for business continuity purposes should copy in your work account to ensure that the council has an appropriate record of its business. Council data must be deleted from personal equipment and email accounts as soon as the necessity to use personal equipment is over.

It is expected that users will prepare for expected events such as tube strikes or forecast bad weather and take equipment home with the approval of their line manager if it is expected that attendance at work would not be possible.

2.6 Social media

The Council’s Social Media Policy provides a framework for the effective, compliant and secure use of social media to promote and develop the council’s objectives, services and achievements; providing information about council services to service users. It provides guidance to staff on best practice when using the medium in a professional capacity whilst protecting the reputation of the council and allowing the safe and controlled roll-out of social media across the organisation.

Specifically for Members, the council will support the use of social media by Members in their committee roles. It will provide advice on the establishment of an account by any Member of the Council. Council officers cannot support the use of any medium for party political matters. Committee Members should use ‘Cllr’ accounts for party political issues. Members should always keep clear distinctions between council business, political business and personal business. It is recommended that Members have separate accounts for different roles.

2.7 User responsibilities for the care of ICT equipment

You must immediately report any loss or disposal of council ICT equipment to your line manager, the Information Management team on x2029, Insurance on x7197 and the IT service desk on 020 8359 3333 during office hours.

2.8 Software installation

Users must not install any software on council machines unless authorised to do so by IS. Any requirement for software should be requested through the IT service desk.

Council software must not be loaded onto non-council devices.

2.9 Fault reporting

All IT faults and IT security issues should be reported to the IT service desk.

The Service Desk is open between 8am and 6pm, Monday to Friday.

Telephone extension x3333 or email ITservicedesk@barnet.gov.uk.

3. Email Services

The email system is provided to assist users in the execution of their council duties. The email section of this policy applies to both internal and external emails.

3.1 Use of council email system

The use of email should be handled with care; consequently, users should be aware of the following:

- Email auto forwarding to external addresses is forbidden.
- No user must use the council's email system in any way that may be interpreted as insulting, threatening, abusive, disruptive or offensive by any person or company, or anything that may be harmful to council morale or reputation.
- Examples of prohibited material include:
    - Sexually explicit messages, images, cartoons or jokes; unsolicited propositions; profanity, obscenity, slander or libel; ethnic, religious, or racial slurs; political beliefs (acceptable for Members), lobbying or canvassing;
    - Any message that could be construed as harassment or disparagement of others. In particular, but not limited to those based on their sex, race, sexual orientation, age, national origin, disability, religious, or political beliefs.

  - Any message that incites or depicts violence, or describes techniques for criminal or terrorist acts.

- Email communications are not guaranteed to be private, arrive at their destination within a particular time, or at all. Emails are subject to the same laws as other forms of communication, and could render the user and council liable to actions for defamation.

- Email content may be subject to disclosure under the Freedom of Information Act 2000 and the Data Protection Act 1998.

- Users must not send unsolicited, irrelevant or inappropriate email to multiple newsgroups or to mailing lists on the internet.

- The forwarding of chain letters is forbidden. This includes those purporting to be for charity or other good causes. Virus warnings come under the same exclusion and should be discussed with the IT service desk, but should not be forwarded to anyone inside or outside the council.

- Users must not misrepresent themselves or use anonymous mailing services to conceal their identity when mailing through the internet, falsify emails to make them appear to originate from someone else, or provide false information to any internet service which requests name, email address or other details.

- The user logged in at a computer will be considered the author of any messages sent from that computer. Remember to log-out, or lock your computer when you leave your desk. Under no circumstances should you send an email from a device that you have not logged into.

- Attachments in email messages often contain viruses, and will likely appear to come from someone you know. Read the text part first. You can often judge by the language used whether it looks right for the sender. If you feel it is not genuine, do not attempt to open the attachment. Contact the IT service desk for assistance.

- Users should not access emails not intended for them, even if they are not protected by security controls, or do anything which would adversely affect the ability of others to access emails or internet resources that they are entitled to access.

- Be aware that council and 3rd party email systems can and do support proxy (delegate) access to email.

- If sending Sensitive Personal Data (as defined by the Data Protection Act 1998) electronically, a secure email system provided by the council should be used.

- Emails that are sent using GCSx services are required to be protectively marked in accordance with the council's Protective Marking for GCSx Emails Policy

3.2 Best practices for email usage

It is important to recognise that email folders are not a good mechanism for long-term retention of council data. Under the Data Protection Act, the council must not hold data for longer than it is needed. If it is necessary to retain information from an email it should be stored in a more accessible form; if it is not necessary to retain the information it should be deleted:

- All users of email are required to ensure that messages are deleted when the information they contain is no longer required (or has been saved appropriately elsewhere).
- All users of email are required to ensure that information in their mailbox is moved out to a more appropriate form of storage if it must be retained and used by others in the council (eg a document management or case management system). This is especially applicable to attachments or to emails that contain personal information relating to others.
- The use of Personal Folders is not recommended.

3.3 Data Protection and Email

Sensitive Personal Data (as defined by the Data Protection Act 1998) and highly confidential information when sent externally must only be sent via secure email such as GCSx or Encrypt and Send. Users are responsible for considering the sensitivity of data in an email before they send it and choosing the most appropriate method of transfer.

3.4 GCSx Email Accounts

GCSX email accounts should be used for the sending of sensitive personal data. An account can be requested from IS self-service. Users of GCSx email accounts should refer to the council's "Protective Marking for GCSx Emails Policy" before use. GCSx emails can only be sent to other users on the secure PSN network. Where communication is outside the scope of the GCSx system the council alternative secure mail systems should be used.

4. Internet Services

Access to the internet is provided to assist employees in the performance of their council duties. Where access is provided use should be limited to official council business or fall within the guidelines set out in section 2.2.

4.1 Use of council internet services

The use of the internet must be handled with care. Users should be aware of the following:

- In line with the Social Media Policy, staff should not post messages on any internet message boards or other similar web based service that would have an adverse effect on the council or which a reasonable person would consider to be offensive or abusive. The list of prohibited material is the same as those for email listed in 3.1.
- As part of routine security measures, all websites visited are centrally logged. The council monitors and logs all internet accesses by individuals and reserves the right to access and report on this information.
- You should not visit websites that display material of a pornographic nature, or which contain material that may be considered offensive. It is recognised that you may accidentally open a site which has such material, if this happens you should contact the IT service desk immediately.
- You should not enter your work email address on a website except on council business approved by your line manager.
- The person logged onto a computer will be considered to be the person browsing the internet. You must log out or lock your computer when leaving your desk to ensure that no unauthorised use of your computer can take place. Under no circumstances should you browse the internet, or use systems, from a computer that you have not logged into.
- You should not use unauthorised cloud storage such as DropBox, Google Docs and similar applications for council data without permission from IS or IMT.

4.2 Anti-virus

Users must not recklessly introduce a computer virus or malicious code into council computers. Deliberate introduction or transmission of any virus, or software designed for breaching security controls or creating computer viruses is an offence under the Computer Misuse Act 1990. A policy of virus checking on all executable code sent by electronic means is in place. Virus protection software is installed on all council computer equipment:

- No attempt should be made to bypass or disable the virus protection, or to turn off or delay the periodic updates.
- Any employee who suspects that his/her workstation or laptop has been infected by a virus or malicious code must immediately call the IT service

desk, disconnect the device from the council network and stop using the computer.

- All internet emails and their attachments received and sent by the council's network are virus checked and encrypted mail will be blocked if it cannot be virus checked.
- Do not follow unsolicited links including those received via email, web fora etc.
- Any employee recklessly transmitting a virus or malicious code to or from council computers is in breach of this policy.
- Incoming media shall be scanned for viruses before they are read. Employees shall only load media under approval from the IS department.

5. Systems Use

5.1 Systems Access

Line/Hiring managers should ensure that all new users have the correct access at the appropriate level to any systems they may require to effectively carry out their role. They must also ensure that users do not have access to any personal or sensitive data that is not required, as this would be breach of the Data Protection Act.

Information Services, in consultation with the Governance Team within the Assurance Group, will ensure that Members have the appropriate level of access to effectively carry out their role.

If a user changes role/service their systems access must be reviewed to ensure only appropriate levels of access are available. This is the line/hiring managers responsibility. Similarly, when a user leaves LBB their line/hiring manager is responsible for completing the leaver process/checklist including updating/ceasing this access. The line manager will be held accountable in the event of a data breach resulting from the failure to assure the correct level of access. In the case of Members, this responsibility falls to the Head of Governance.

All users have the responsibility to inform their manager immediately if they become aware that they have access to any records, drives or systems that they do not legitimately require to effectively carry out their role. In the case of Members they should inform the Head of Governance if they become aware that they have access to any records, drives or systems that they do not require to effectively carry out their role.

5.2 Monitoring of Systems Use

The council may, for authorised monitoring purposes, view any system transactions, read any email and attachment drafted, sent or received at work; or view any internet site visits or transactions, in particular to check policy compliance. However, every effort will be made to avoid unnecessary access to content which is clearly marked as ‘personal’, unless those emails form part of an investigation into the use of IT equipment.

Such monitoring and subsequent reports will be restricted to authorised persons. Usage reports measuring frequency and size of emails, sent or received, and the extent and frequency of internet use will be disclosed to authorised users undertaking investigations under this and other information policies. These reports may identify the user, destination or type of site.

System records may also be subject to access requests under Freedom of Information or Data Protection legislation.

Note, at the council’s discretion such information may also be disclosed to specialist 3rd parties as part of LBB’s own computer forensics investigations.

In addition, it may be necessary to access users’ emails in order to prevent or detect crime, establish the existence of facts relevant to the council (e.g. gather evidence of a business transaction), to ascertain compliance with regulatory practices relevant to council business, disciplinary investigations / employment proceedings or checking for business relevant emails during absence.

If managers require access to a user’s account for business purposes during a user’s absence, this request should be made to the IT service desk.

If a technical problem arises with system content, for example a blocked mail item, it may also become necessary to send that content to a 3rd party for analysis/problem resolution.

6. Copyright Compliance

Information in electronic form may be subject to the Copyright, Designs and Patent Act 1988. This requires that you get permission from the owner of such information before making use of it in any way. The council has a CLA copyright license which permits employees (which includes temporary staff and contractors) to download, copy and reuse copyrighted material subject to license conditions. These can be found in the council’s Copyright Policy.

The CLA license only covers council employees and therefore does not cover employees of CSG and Re, or Members. See the Council’s Copyright Policy for more information.

Users should not copy information originated by others and re-post it without permission from, or at least acknowledgement of, the original source, even if the content is modified to some extent. Users should not assume that information posted on the internet actually originates from the person or organisation that appears to have produced it without some form of authentication.

Copyright and other rights in all messages posted on the internet from a council account, such as material produced at work, belongs to the council, and not to users personally.

If in doubt about copyright issues you should refer to the council's Copyright Policy.

7. Review of the Acceptable Use Policy

This policy will be reviewed on an annual basis or as required by policy or legislation changes.

8. Contact Information/Further Guidance

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

Address: London Borough of Barnet
Building 4
North London Business Park
Oakleigh Road South
London N11 1NP

Tel No: (020) 8359 3333
Email: ITServicedesk@barnet.gov.uk

Tel No : (020) 8359 2029
Emails : data.protection@barnet.gov.uk

This page is intentionally left blank

Customer and Support Group (CSG)

LBB BlackBerry Policy

Table of Contents

Introduction

This policy applies to all Members, employees, temporary employees and contractors working for the London Borough of Barnet (LBB) and issued with BlackBerry devices. It describes the rules governing the use of such devices.

LBB allows usage as part of a user's normal business processes; however care needs to be taken over use of a BlackBerry, as it could possibly allow unauthorised access to LBB systems and data.

Devices are provided by LBB Primarily for LBB use; but limited access for personal use is allowed. Enhanced use for personal calls is allowed as long as you subscribe to the LBB personal call plan.

Further information about the use of computer equipment provided by LBB is provided in the Acceptable Use Policy.

Scope

The controls set out in this document apply to all user accounts.

Policy

All LBB supplied BlackBerrys and content remains the property of LBB and is subject to regular audit and monitoring. These devices must only be connected to a LBB Laptop or desktop.

Users must be aware that the device contains or provides access to the LBB data; as such users must take appropriate action to protect the device from being lost or stolen. Under no circumstances should the blackberry be disposed of, all devices should be returned to LBB for safe disposal.

Only devices which have been built to LBB Standards can be attached to the LBB data network either directly or through a LBB owned or leased network, PC or laptop. This will ensure the appropriate security controls are in place

All BlackBerrys have been preconfigured with security to conform to *PSN Requirements*

Once received the user is not authorised to change any security settings.

A brief overview of security settings applied to the devices are given below

- 256 Bit AES Encryption
- No Bluetooth connectivity
- No WiFi connectivity
- No Blackberry Messaging service (BBM)

- Forwarding emails to personal e-mail accounts is not allowed.
- A 9 character password length which must include numeric characters (At least one uppercase alpha, 1 lowercase alpha, 1 numeric and 1 special character)
- 12 month password history (this means that you cannot use the previous 12 passwords).
- The user will receive a message to change the password every 30 days, on the screen of the BlackBerry.
- 5 incorrect passwords attempts are allowed, following this the device automatically wipes.
- The BlackBerry screen with go black after 30 seconds of inactivity; this is for power save.
- The multimedia card is encrypted with your BlackBerry password. The multimedia card will be automatically erased when the BlackBerry is erased e.g. after 5 incorrect password attempts.
- The BlackBerry will lock after 5 minutes of inactivity.
- Sim Card content protection is activated: When receiving a call on your BlackBerry, if the person calling is in your contacts the caller's name will only be visible when your BlackBerry is unlocked. If the BlackBerry is locked only the number will be visible on the screen.

Internet Browsing

Limited internet browsing is allowed on your BlackBerry and is passed through Barnet Infrastructure and Websense Servers for monitoring.

Taking Your BlackBerry Abroad

Your manager must authorise you to take your BlackBerry abroad on business. If the situation arises in which Members need to take their device out of the UK they must first check with IS if this is appropriate. Taking devices outside the UK may put council information and the council network at risk. Some countries are banned from connecting to Public Services Network connected networks. Certain countries may confiscate encrypted devices on entry and / or force a user to enter passwords and bypass security. Confiscated devices may not be returned.

Please contact the ITservice desk (ITservicedesk@barnet.gov.uk; 020 8359 3333)to have roaming enabled on your device.

Use of Camera on BlackBerrys

BlackBerrys enabled with cameras should primarily be used for taking business related pictures however, some limited personal use is allowed, but storage should not interfere with LBB business use.

Pictures can only be downloaded to a secure device LBB computer (laptop or desktop) and removed from the device as soon as possible. This is not enabled on a LBB PC and requires a signed exception form and business case.

Only take pictures of individuals with their permission to do so, or follow current policy where this is impractical.

Costs and charging

Costs incurred are charged against your departmental cost centre, and charges will be detailed against the BlackBerry mobile number.

Personal calls are allowed as long as you subscribe to the LBB personal call plan; contact the IT servicedesk for further information (ITservicedesk@barnet.gov.uk; 020 8359 3333) for further information.

Damaged Devices

If your device has been accidentally or maliciously damaged, this must be reported In line with the lost or stolen process document as soon as reasonably possible to the following:

- In person to the police and a crime reference number obtained
- To your manager or for Members to the Head of Governance to administer
- The LBB service desk will provide you with a mobile device claim form, this needs to be completed with the crime reference number, a copy of the form should go to your manager for staff or Head of Governance for Members.
- A copy of the LBB Insurance form should also be sent to the LBB insurance team to request a replacement device.

Note: this process applies to damage through accidental or malicious act. It does not apply to damage over time through normal use or wear and tear.

Barnet Council Public Services Network (PSN) Acceptable Use Statement

This form must be signed by the employee before a GCSx mailbox is created for their use.

I understand and agree to comply with the information security rules for the use of PSN secure services supplied by Barnet Council.

(These rules are in addition to any other information management policies in force at Barnet Council at any time.)

The security rules relating to PSN usage include:

- I acknowledge that my use of the PSN may be monitored and/or recorded for lawful purposes;
- I agree to be responsible for any use by me of the PSN using my unique user credentials (user ID and password, access token or other mechanism as provided) and email address;
- I will not use a colleague's credentials to access the PSN and will equally ensure that my credentials are not shared and are protected against misuse;
- I will protect such credentials at least to the same level of Protective Marking as the information they may be used to access, (in particular, I will not write down or share my password other than for the purposes of placing a secured copy in a secure location at my employer's premises);
- I will not attempt to access the PSN other than from IT systems and locations which I have been explicitly authorised to use for this purpose;
- I will not transmit information via the PSN that I know, suspect or have been advised is of a higher level of sensitivity than my PSN domain is designed to carry;
- I will not transmit information via the PSN that I know or suspect to be unacceptable within the context and purpose for which it is being communicated;
- I will not make false claims or denials relating to my use of the PSN (e.g. falsely denying that an email had been sent or received);
- I will protect any material, whatever the sensitivity or protective marking, sent, received, stored or processed by me via the PSN to the same level as I would paper copies of similar material;
- I will not send information marked RESTRICTED or above over public networks such as the internet unless approved encryption has been applied to it;
- I will always check that the recipients of email messages are correct so that potentially sensitive or protectively marked information is not accidentally released into the public domain;
- I will not auto-forward email from my PSN account to any non-PSN email account;
- I will not forward or disclose any sensitive or protectively marked material received via the PSN unless the recipient(s) can be trusted to handle the material securely according to its sensitivity and forwarding is via a suitably secure communication channel;

- I will seek to prevent inadvertent disclosure of sensitive or protectively marked information by avoiding being overlooked when working, by taking care when printing information received via the PSN (e.g. by using printers in secure locations or collecting printouts immediately they are printed, checking that there is no interleaving of printouts, etc.) and by carefully checking the distribution list for any material to be transmitted
- I will securely store or destroy any PSN printed material;
- I will not leave my computer unattended in such a state as to risk unauthorised disclosure of information sent or received via the PSN (this might be by closing the email program, logging-off from the computer, activating a password-protected screensaver, etc., so as to require a user logon for activation); and
- Where Barnet Council has implemented other measures to prevent unauthorised viewing of information displayed on IT systems (such as an inactivity timeout that causes the screen to be blanked or to display a screensaver or similar, requiring a user logon for reactivation), then I will not attempt to disable such protection;
- I will not knowingly introduce viruses, Trojan horses or other malware into the system or PSN;
- I will comply with the Data Protection Act 1998 and any other legal, statutory or contractual obligations that my employer informs me are relevant; and
- [For a member of staff] If I am about to leave Barnet Council's employment, I will inform my manager prior to departure of any important information held in my account.
- [For a Member of the Council] I will inform the Head of Governance of my intention to resign from office who will authorise the closure of my account.

I accept the above terms and conditions of use for the PSN

Signature ………………………………………….

Print Name ………………………………………….

Service Area ……………………………………………

Date …………………………………………….