AGENDA ITEM 5

BLACKBURN with DARWEN BOROUGH COUNCIL

REPORT OF:	**The Director of ITM&G**
TO:	**The Members' Standards Committee**
ON:	**3rd July 2014**

SUBJECT IT Acceptable Use Policy

1. PURPOSE OF THE REPORT

To advise the committee of the requirement that all elected members comply with the Council's IT Acceptable Use Policy (the AUP) in order that the Council complies with various Central Government regulations. Also, to provide members with updated advice and guidance related to their obligations under the Data Protection Act, the Freedom of Information Act and the Environmental Information Regulations.

2. OPTIONS

None

3. RECOMMENDATIONS

To approve the introduction and distribution of the AUP and the guidance document to all members.

4. BACKGROUND

The Council is extending the number of services it delivers by digital means and all members and officers are increasingly reliant on the council's ICT services. The AUP defines what constitutes acceptable use of the Council's IT systems to ensure that they are used legally, ethically, and that their use supports aims, values and objectives of the Council.

5. RATIONALE

The council's increased reliance on the use of ICT systems for service delivery brings with it various risks, both reputational and financial. As part of the governance framework set up to manage and mitigate those risks, the Council devised the AUP to inform users what is acceptable when using the Council's IT systems and their personal responsibilities.

6. POLICY IMPLICATIONS

The AUP sets out the governance framework for the use of the Council's ICT systems, and provide the foundations for legal, ethical and effective delivery of ICT services across the Council. The guidance provides Members with a valuable information

resource to assist them to understand their obligations under current legislation and regulations.

7. FINANCIAL IMPLICATIONS

There is a risk that an inability to provide evidence of compliance with an AUP could be discourages partners from sharing digital services with the Council, to the detriment of citizens.

8. LEGAL IMPLICATIONS

None. However, the Public Services Network (PSN) code of connection and the NHS Information Governance Toolkit both demand that public sector bodies have comprehensive and robust ICT governance and compliance frameworks in place that assure the security and integrity of the information we generate, use, store and share.

9. RESOURCE IMPLICATIONS

None.

10. EQUALITY IMPLICATIONS

Equality impact assessments were carried out when the AUP was originally approved in 2010.

11. CONSULTATIONS

Chief Officer/Member

Contact Officer:	Shane Agnew, Head of IT Strategy and Operations
Date:	24th June 2014
Background Papers:	Acceptable Use Policy Version 1.10
	Access to Information – Guidance for Councillors V1.3

Policy Document

IT Acceptable Usage Policy

1st December 2010

1 Purpose

The purpose of this policy is to:

- Define the acceptable use of Blackburn with Darwen Borough Council's IT Systems
- Ensure all use of the Council IT Systems is legal, ethical, and consistent with the aims, values and objectives of the Council
- Inform all users of what they can and cannot do
- Inform all users of their personal responsibilities when using the Council's IT Systems

2 Scope

This policy applies to all people using or accessing Blackburn with Darwen Borough Council IT Systems and must be adhered to whenever using or accessing those systems.

3 What you should know

It is your responsibility to familiarise yourself with this policy and ensure you comply with its requirements.

You must have read, understood and accepted the terms of this policy before using or accessing the Council's IT systems/facilities.

You are responsible for the information you view, copy, forward or write when using or accessing all Council systems, the internet and other networks you may have access to.

- You must ensure the information you use is appropriate to the work you do

- You can do so by following the rules set out in this policy along with use of your own judgement. If you are in any doubt whether something is acceptable, ask your line manager or Head of Service

All systems will be monitored and/or recorded. Use of systems is therefore not private and data may be shared as necessary to establish if this policy is breached

Any breaches will be subject to Blackburn with Darwen Borough Council's disciplinary procedure. If a criminal offence is considered to have been committed further action may be taken to assist in any investigation and/or prosecution.

4 How to obtain further information

Further information is available in the form of guidance notes which can be found on the Council's intranet.

5 IT Access

Information is an important and valuable asset of the Council which must be protected against accidental or malicious disclosure, modification or destruction. The Council also has a number of obligations resulting from of Acts of Parliament and other legally binding requirements.

As such, access controls are put in place to ensure the Council's information is safe and that it has met its obligations.

- Each user will be provided with a personal login (a User ID and associated password) for the Council's IT Systems
    - Users must not share their login details with anybody else
    - Users must only use their own User ID and password – it is forbidden to share or use another user's login details
    - Users must keep their passwords safe and private:
        - Passwords must not be written down or stored on a computer system
        - Passwords must not be disclosed to anyone else
    - Passwords must be changed on a regular basis.
    - Users must change their password immediately, and report this to the IT M & G Service desk, if they suspect that it known by somebody else,
    - Users must always lock their computer when leaving it unattended.
- Only use authorised equipment and do not tamper with it
    - Only use equipment approved by the Council to record, process or store data relating to Council business:
        - Unless specifically authorised by IT M & G, all IT equipment must be sourced from IT M & G
        - Home computers must not be used to access Council systems except as authorised by IT M & G. A list of applications which users are authorised accessed from their home computers (such as Webmail) will be published on the Council's intranet
        - Unencrypted USB Flash drives (sometimes referred to as memory sticks) must not be used to save any personal, sensitive or confidential data
        - Users must only use USB Flash drives that have been encrypted using the Council's encryption facilities
        - Data on encrypted USB flash drives must not be copied to or saved on non BWD IT equipment
        - Certain applications may require access via 3rd party equipment – this will be agreed by IT M & G on a case by case basis

- Users must not plug in any non-Council equipment (such as printers, cameras, iPods, MP3 players, phones or other USB devices) to Council IT systems, unless specifically authorised to do so by IT M & G

- Users must not attempt to disable or re-configure IT equipment security measures. Authorised equipment is set-up, by IT M & G to ensure the most appropriate level of security

- Users must not install any software onto Council IT equipment.

- Users must take all reasonable care of any IT equipment issued to them and must return it in good condition

- Any equipment that is surplus to requirements must be returned to IT M & G for reassignment or disposal in a controlled manner that includes the removal all software and data and the management of the Council's IT assets

  - Users must not store surplus equipment 'just in case it might be needed'; its security configurations quickly become out of date and may render the system vulnerable to un-authorised access

  - Users must not 'pass on' equipment to other users or departments. It is the responsibility of IT M & G to manage the Council's IT assets and issue all IT equipment

  - Equipment that has not been used for three months will be prevented from accessing the Council network.

- Users of authorised portable digital equipment, including cameras, encrypted USB flash drives and mobile phones, must keep it secure at all times:

  - Ensure equipment is not left unattended unless it is locked away securely

  - Users must only remove equipment from Council premises if authorised to do so by a Head of Service or Chief Officer.

- Connecting to the Council's systems whilst abroad carries additional security risks, so there are additional restrictions if you need to work outside the UK.

  - Webmail access must not be attempted from outside the EEA.

  - Users must not take Council IT equipment abroad unless they have approval from their Director and IT M & G.

- Access to Internet sites is restricted by the system but it is the individual user's responsibility to ensure that they do not visit restricted sites or view inappropriate content including:
  - Pornographic or other 'unsuitable' material that might be deemed illegal, obscene or offensive.

  - Sites containing violence, hate and discrimination, weapons or bomb making.

- Users must not post statements on the internet that are defamatory, or information that is false, misleading or breaches confidentiality concerning the Council, persons associated with the Council or any other organisation or person (this includes, but is not limited to, text, videos, images, sound.).

- If a user's job role requires them to access information held on inappropriate or restricted internet sites, written approval must be obtained from the user's Head of Service and submitted to IT M & G, prior to access.

- The Council reserves the right to grant access for another member of staff to view your files and emails. This would only be done following approval by a Chief Officer.

6 Use for activities not related to Council business

The Council's IT Systems are provided for the purpose of conducting and supporting official business activities; however the Council permits 'occasional and short' personal use. That personal use must not:

- Interfere with or interrupt in any way, your job, other users or Council business in general
- Bring the Council into disrepute
- Involve accessing restricted sites or viewing inappropriate content, as noted above
- Reduce the security of the Council's IT systems or increase the chance of a security breach
- Involve access to on-line banking or other on-line financial transactions (including on-line purchasing)
- Have the potential for financial gain either personally, for an acquaintance or as a business (this includes visiting gambling or money making sites and using Council systems to run a private business venture).
    - The staff intranet marketplace is specifically excluded from this provision and may be used by staff.
    - Where the Council makes other sites available via the Council intranet, these will also be exempt from this provision.
- Result in the storage of personal information (including photographs) on Council owned or managed storage devices

The Council will be the arbiter of whether or not the 'occasional and short' use was reasonable in the circumstances.

For guidance, occasional and short will generally mean the following:

Occasional: Once or twice a day for a short period.

Short: In the user's own time, use for a few minutes and preferably not at lunchtime.

7 Email

Email has the same legal status as a Council letter, memo or fax and, therefore the emails that users produce, send and receive are the property of the Council.

It should also be noted that emails and attachments may need to be disclosed under the Data Protection Act 1998 and the Freedom of Information Act 2000.

- Emails used to conduct or support Council business must be sent using the official Council email system (e.g. firstname.lastname@blackburn.gov.uk).
- Non-work email accounts must not be used to conduct Council business.
- Users must not send or circulate any material that is designed or likely to cause annoyance, inconvenience or needless anxiety to any person.
- Emails must not contain indecent, obscene or libellous material, material likely to cause offence or any material which harasses any other employee or 3rd party on the basis of sex, race, religious or political beliefs, marital status, disability, age or sexual orientation.
- Users must not create or transmit material that includes false claims of a deceptive nature.
- Email must not be used to conduct illegal activities, gambling or soliciting for personal profit. For the avoidance of doubt, requests for payments such as donations or sponsorships are not classed as personal profit.
- Users must not create or transmit chain letters or jokes, or such material that infringes the copyright of another person or organisation including intellectual property rights.
- Any user who receives any emails from outside the Council containing items which are prohibited by this policy should immediately delete that email. If such emails continue to be received, the user should report it to their line manager.
- Any user who receives an email from another BwD Council email account, which contains items that are prohibited by this policy, should keep that email and contact report the breach as defined in section 10 below.
- If a user receives any other type of email that causes concern, they should seek the advice of management.
- Users must not transmit by email any file attachments which are known to be infected with a virus, or any other sort of malicious software (known as malware), furthermore:
    - Users must not download data or programs of any nature from unknown sources,
    - Users must notify IT M & G of any virus warnings that occur while using any Council IT system.
- Users must not set-up auto-forwarding of any email.
- Emails containing personal, confidential or sensitive information (therefore classified as PROTECT or RESTRICTED information) **must not** be forwarded to **any** personal email address.
- When sending or receiving emails containing RESTRICTED information:
    - Users should always use a GC Mail account when communicating with other users of the GCSx or any connected network (e.g. other public sector workers).
    - Users should send appropriately encrypted emails from their standard Council email accounts when communicating with recipients outside the Council who do not have a GC Mail account. Users should contact IT M & G if they need to send encrypted emails.

Users who have a regular requirement to send PROTECT or RESTRICTED content emails to recipients who have GC Mail addresses, should request a GCSx email account through their Head of Service.

7.1 Bulk email – email to more than 25 people outside the Council

Users needing to send bulk emails must contact the Council's Communications and Marketing team. These cannot be sent via the normal email system because they will be regarded as SPAM and breach the agreement with the Council's email provider.

Use of bulk email requires compliance with the same security rules listed above, which must be adhered to at all times. In addition the Communications and Marketing team may impose additional restrictions on the use of bulk email.

8 Social Media

Above and beyond the instructions and policy statements contained within this document, there is specific guidance on the use of social media. All users should read that guidance carefully before using any social media such as Twitter, Facebook, MySpace, Forums, etc.

9 Software & other copyright material

To ensure that the Council complies with the Copyright, Designs and Patents Act 1998, the following rules must be adhered to:

- All software must be acquired, installed and appropriately licensed through IT M & G, including all commercial, shareware, freeware, and any other public domain software.
- Games, wallpapers and screensavers must not be loaded onto Council IT systems.
- The Council expressly prohibits the illegal duplication of any software and/or copyright material.
- Copying, downloading and storing of copyrighted material (such as music, and photographs from magazines) on to Council IT equipment is strictly prohibited.

Please be aware that failure to follow this policy could lead to criminal prosecution.

10 Security & reporting breaches

It is the responsibility of all employees and users to immediately report to the IT M & G Service Desk by phoning 01254 585279:

- The loss or theft of any Council owned IT equipment or electronic devices such as mobile phones, cameras and memory sticks.
- Any known or suspected breaches of this policy.
- Any actual or suspected breaches in information security.

- Any misuse or irresponsible actions that affect business data or Council owned IT equipment.

Document Control

Organisation	Blackburn with Darwen Borough Council
Title	IT Acceptable Usage Policy
Author	Sarah Slater
Filename	IT AUP-v1.10
Document Owner	Strategic Director of Resources
Document Administrator	IT M & G Commercial & Compliance
Subject	IT Acceptable Usage Policy
Protective Marking	Unclassified
Review date	05/07/13

Revision History

Revision Date	Revised by	Previous Version	Description of Revision
03/06/10	Neil Smith	V1.01	Feedback from staff, HR, Audit & Assurance and Communications
08/06/10	Neil Smith	V1.02	Further feedback from staff, HR, Audit & Assurance and Communications
11/06/10	Neil Smith	V1.03	Further feedback from staff, HR, Audit & Assurance and Communications
29/06/10	Neil Smith	V1.04	Feedback following comments from Capita HR and Civil Contingencies
19/08/10	Neil Smith	V1.05	Feedback from IGS working group meeting on 18th August 2010
19/08/10	Neil Smith	V1.06	Feedback from IGS working group meeting on 18th August 2010
24/10/10	Sarah Slater	V1.07	Feedback from IGS working group and Policy Working Group
30/11/10	Gary Ennis	V1.08	Updated following feedback
08/12/10	Mike Zammit	V1.09	Updated following review by Director of IT M & G
05/07/13	Chris Daniels	V1.10	Minor update to reflect department name change.

Document Approvals

This document requires the following approvals:

Sponsor Approval	Name	Date
Strategic Director of Resources / SIRO	Denise Park	
IT M & G Director	Mike Zammit	08/12/2010
Strategic HR Director	David Fairclough	31/01/2011
CESG		
LJNCC	Ros Billingham	18/02/2011
Executive Board		

Document Distribution

This document will be distributed to everyone with a domain login to the Council's network.

APPENDIX1

I have read and accept the Blackburn with Darwen Borough Council IT Acceptable Usage Policy.

User Name: ..... Department.....

User Signature.....Date.....

Payroll ID.....

Note: Any updates to this policy will require all user's to re-sign (and as necessary go through updated training) before continuing to access the Council's IT Systems.

ITM&G Information Governance

Access to Information

Guidance for Councillors

17

CIRCULATION LIST

For Consultation	Date Reviewed
ITM&G EMT	20/05/2014

RELATED DOCUMENTATION

Title	Version	Date
Data Protection Policy POL010 http://www.blackburn.gov.uk/Pages/Data-protection-policy.aspx	V1.0	13/08/2012
Freedom of Information Policy POL012 http://www.blackburn.gov.uk/Pages/Freedom-of-information-policy.aspx	V1.0	13/08/2012
Records Management Policy and Data Retention Schedule POL011 http://cms.intra.blackburn.gov.uk/server.php?show=ConWebDoc.57463	V2.03	27/06/2013
Acceptable Use Policy POL001 http://cms.intra.blackburn.gov.uk/upload/pdf/IT_AUP-v1_10_20130710153700.pdf	V1.10	01/12/2010

VERSION CONTROL

Version	Date	Author	Comments
1.0	20/11/2011	AGMA	Draft Created
1.1	01/03/2013	Sarah Slater	Guidance Refresh
1.2	20/05/2014	Sarah Slater	Guidance Refresh
1.3	24/06/2014	Sarah Slater	Guidance Refresh

AUTHORISED BY

Sponsor Approval	Name	Date
ITM&G Director/SIRO	Mike Zammit	**May 2014**

Document Distribution	All Elected Members, IG Officers, IG Departmental Representatives, Democratic Services Officers
Guidance Review Date	May 2015

Contents

Introduction

This guidance is aimed at assisting Councillors in respect of access to information mainly in respect of the Freedom of Information Act 2000, [FOIA] and other regimes such as the Data Protection Act 1998 [DPA].

It may also be a useful guide for officers who may advise Councillors.

These issues are relevant to the understanding of this guide: -

- Councillors can make FOIA requests themselves and also on behalf of constituents.
- The definition of a local authority, within the Freedom of Information Act is adapted from the Local Government Act 1972 and therefore includes Councillors.
- Elected Councillors have all the rights of access available to members of the public and some additional rights.
- Under the Data Protection Act 1998, Elected Councillors need to consider that when using personal information for any particular purpose, they take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.

Overview of the Freedom of Information Act 2000

The Act came into force in two stages; the first stage was the approval of the Publication Schemes for each authority in 2003.

In 2005, the rights of access were brought in across all the authorities - this was the second stage.

FOIA establishes two mechanisms for placing information in the public domain. Firstly, it establishes a right for any person making a request to a public authority to be informed in writing whether or not the authority holds that information and secondly, if so, to have access to the information subject to any exemption and costs limits.

The authority must publish and maintain a Publication Scheme (http://www.blackburn.gov.uk/Pages/Publication-scheme.aspx) and also establish a fees structure.

Two codes of practice in respect of FOIA have been issued by the Information Commissioner's Office. One is known as the Section 45 Code (1) and the other is known as the Section 46 Code (2)

Within the Act, are exemptions to the disclosure of information - these can be absolute or qualified and where a qualified exemption applies, the authority must apply a public interest test.

The Information Commissioner's Office has powers to guide and promote the good practice and observance by public authorities and he can issue practice directions, decision notices, information notices and enforcement notices.

The First Tier Tribunal (Information Rights) hears appeals in respect of notices issued by the Information Commissioner.

---

[1] Code of Practice on the discharge of public authorities functions under Part1 Section 45 of the Freedom of Information Act 2000 issued November 2004

[2] Code of Practice on the Management of Records issued under section 46 of the Freedom of Information Act 2000 issued November 2002

Information Held

For the purposes of the FOIA, information is held by the Council if:-

- It is held by the Council, otherwise than on behalf of another person, or;
- It is held by another person on behalf of the authority.

Information which has been created by the Council is subject to FOIA, provided that:-

- it retains possession of that information or,
- the information has been provided to another public authority or,
- the information is held on behalf of the originating public authority by a third party.

All recorded information e.g. letters, emails, reports, videos, CCTV etc. is covered

Information held by Councillors

This is held in three distinct ways: -

1. Political Activities

This information may be outside the scope of FOIA.
Information, even though it may be held "on a Council system" whether it is paper, electronic or otherwise, it may be "held on behalf of."

Members are reminded of the Code of Conduct extract as follows: -

"b) must, when using or authorising the use by others of the resources of Blackburn with Darwen Council,

(i) act in accordance with Blackburn with Darwen Council's reasonable requirements;

(ii) ensure that such resources are not used improperly for political purposes (including party political purposes); and

(iii) must have regard to any applicable Local Authority Code of Publicity made under the Local Government Act 1986."

If Councillors are unsure in this respect they should seek the advice of the monitoring officer (Director of HR and Legal Services)

2. Ward Activities

By nature of the Councillors' ward activities - some of this information, if it is personal information, will fall under the **Data Protection Act 1998**, but some may be considered as part of the Council's information and will fall under the FOIA.

People can ask for information about constituency casework, but this is not always classed as Council information because in many cases the matter will not be referred on to the Council - in which case the information remains the Councillor's responsibility.

If the matter is then raised with a Council official, and that official records the information, it then becomes Council information, which may be disclosable – (exemptions may then apply particularly where personal information is involved).

If a person is asking about details of their own case then this is likely to be an enquiry under the Data Protection Act 1998, rather than FOIA.

If you as a Councillor wish to represent a constituent in relation to a subject access request under the Data Protection Act, or to act on their behalf in relation to a Council matter where personal detail will need to be disclosed, it is important to establish that you have consent to act on their behalf.

Information Governance will request to see a signed Form of Authority that issues explicit consent from the Data Subject to disclose their personal information to you. A template is attached.

Form of Authority
Consent to disclose

3. Council Business

In respect of conducting Council business, this is within the scope of FOIA.

This type of information will include the following: -

- Information supplied by officers to Councillors via
  - committees
  - cabinet
  - panels
  - advisory bodies

In respect of Key Decisions:-

- Officer briefings.
- Information, which has been generated by the Councillor and relates to Council business.
- Information generated by officers where support to a Councillor has been provided.
- Information relating to a Decision once that Decision has been taken.
- Personal comments which are made on reports or email that are formally submitted via committee chairs or to officers.

The Local Government Act 1972, [Schedule 12A], in respect of the Access to Information rules, determines what information can legally be withheld in committee reports and meetings. This is referred to later in this guide.

Overview of the Data Protection Act 1998

The Data Protection Act regulates the holding and processing of personal information that relates to living individuals and which is held on computer or, in some cases, on paper.

Organisations or individuals that process personal information covered by the Act may need to notify the Commissioner about their processing. A description of the processing activities is placed on a public register of notifications. These organisations or individuals must also comply with eight data protection principles which together form a framework for the proper handling of personal information. Individuals whose personal information is processed have rights under the Act, for example, to a copy of the information that is held about them.

Notification
In considering whether they need to notify, elected members must first decide in which role they are processing personal information.

1. As members of the Council
2. As a representative of the residents of their ward
3. As a representative of a political party

ICO notification for Elected Members will be carried out by the Information Governance Team. For any further queries relating to notification, please contact the Information Governance Manager on 01254 585226.

Use of Personal Information
When elected members consider using personal information for any particular purpose, they should take into account the context in which that information was collected to decide whether their use of the information will be fair and lawful.

- Personal information held by the local authority should not be used for political or representational purposes unless both the local authority and the individuals concerned agree. It would not be possible to use a list of the users of a particular local authority service, for electioneering purposes without their consent. An example would be using a local authority list of library users to canvass for re-election on the grounds that the member had previously opposed the closure of local libraries.

- When campaigning for election as the representative of a political party, candidates can use personal information, such as mailing lists, held by their parties. However, personal information they hold as elected members for casework should not be disclosed to the political party without the consent of the individual.

- Candidates for election should also be aware of the requirements of the Privacy and Electronic Communication (EC Directive) Regulations 2003 that regulate unsolicited electronic marketing messages sent by telephone, fax, email or text.

Protecting Information

The Council offer guidance on the importance of protecting the Council's Information assets. This is located on a dedicated Information Governance Intranet site:
http://cms.intra.blackburn.gov.uk/server.php?show=ConWebDoc.57463

On this site you will find useful information relating to sharing data, secure transfer of personal data, records management, document retention guidelines and Information Governance contact details.

Information Governance request that Councillors complete Level 1 of the Council's Protecting Information training in order to obtain a basic understanding of information security and comply with Council Policy.

http://blackburn.thedevelopmentzone.co.uk/

Acceptable Use Policy (AUP)

The Public Services Network (PSN) is at the heart of one objective of the government's ICT Strategy. PSN provides an assured network over which government can safely share services, including many G-Cloud services, to collaborate in new ways, more effectively and efficiently than ever before.

In order to continue connectivity with Central Government Services, the Council must produce evidence that demonstrates compliance with appropriate technical security measures. One area of this compliance is the introduction of mandatory Acceptable Use Policies for all users of Council Network Services, in order to mitigate risk to the security and integrity of the Council's Information Assets.

All members of staff within Blackburn with Darwen Council that connect to network services are mandated to comply with the Corporate Acceptable Use Policy (AUP). ITM&G have extended this mandatory compliance with the AUP for all Members in order that the Council can continue to comply with the Central Governments code of connection via the Public Services Network (PSN).

ITM&G will ensure there is an auditable compliance to this policy with the introduction of Metacompliance, a software tool that enables policy acceptance via the Members network connection on their Tablet/Laptop/Desktop.

Membership of other Organisations

Councillors are often appointed to other organisations for example joint working groups. If the Councillor is acting in an official capacity on behalf of the Council then that information held about that activity may fall under FOIA.

Councillors acting in a Non-Council capacity for example as a member of a charity this would not be classed as Council information.

Councillors dealing with FOIA Requests – Best Practice

Councillors are encouraged to generate and handle information according to accepted best practice, which includes: -

- Being objective and making statements that can be substantiated.
- Ensuring that information is only retained for as long as it provides value and destroyed in accordance with recommended Record Retention and Disposal Schedules.
- Knowing how to identify requests for information and what to do with them.
- Knowing where to get advice when it is needed.
- Keeping information up to date.

It is important to note the following: -

- Each request should be handled on a case-by-case basis.
- Requests should be acknowledged within 24 hours
- Requests must be responded to within 20 working days
- FOIA requests received by Councillors intended for the Council should be sent to the appropriate officer/s in Information Governance, G Floor, Tower Black, Town Hall or forwarded to Accesstoinformation@blackburn.gov.uk
- Where Councillors hold information, which is part of a request received by an officer, the appropriate officer will request the information from the Councillor.
- Most requests will be satisfied from Council records.
- In some cases, Councillors will need to decide what information meets the criteria of each request that they hold prior to the submission to the appropriate officer - Councillors may, if they wish, rely on appropriate officers to assist them with this task.
- If documents are to be released, these may be edited to remove information, which does not meet the requirements of the request.
- All relevant information held is required to be passed to Information Governance Officers. They will then apply any redaction/relevant exemptions to disclosure in accordance with the legislation.
- It is an offence under Section 77 of the Freedom of Information Act 2000 where a request for information has been made to a public authority to alter, deface, block, erase, destroy or conceal any record held by the public authority with the intention of preventing disclosure.
- Councillors are reminded of the Members' Code of Conduct.

Environmental Information Regulations 2004 (EIRs)

Environmental Information Regulations came into force in January 2005. The Code of Practice that accompanies these regulations aims to facilitate the disclosure of information under the EIR's by setting out good practice to proactively disseminate environmental information. There will always a presumption in favour of disclosing environmental information.

The main differences between FOIA and EIR are as follows:

- The range of bodies covered by the EIR is wider to allow for consistency with the EC Directive and covers public utilities, and private companies in the water, waste, transport and energy sectors
- Requests for information need not be in writing
- Information held by a public authority includes holding information on behalf of any other person
- Time limits for responding to a request are the same as for FOIA (20 Working days) however Regulation 7 allows for an extension from 20 – 40 working days for complex and High Volume requests.

- No exception is made for requests that will involve costs in excess of the 'appropriate limit' (18hours). All requests must be dealt with and any charges imposed must be reasonable.

The powers of both the Information Commissioner and The First Tier Tribunal (Information Rights) are the same as above for FOIA.

Local Governments Act 1972 Schedule 12A – Access to Information

These statutory instruments are intended to help to give local authorities a shorter and clearer idea of what information should be treated as exempt information:

- Statutory Instrument 2006 No 88 – The Local Government (Access to information) (Variation) order 2006
- Statutory Instrument 2006 No 87 - The Relevant Authorities (Standards Committee) (Amendment) Regulations 2006
- Statutory Instrument 2006 No 69 – The Local Authorities (Executive Arrangements) (Access to Information) Amendment (England) Regulations 2006

These new regulations took effect from 1 March 2006. It affects access by both the public and by Councillors.

The changes alter part 1 of the Schedule 12A, which describe the categories of information that may be considered exempt from the requirement of the Local Government Act 1972 to make available to the public those papers relating to local authority meetings and access to those meetings.

In addition it is now a requirement to consider a public interest test if an exemption is to be applied, ie, consider if the public interest in the information outweighs the application of the exemption. This mirrors the provisions of FOIA

These changes do not alter the existing 'need to know' rights of Councillors but grant additional rights to inspect documents.

Local Governments Act 1972 Section 100F – Access to Information, additional rights

The Local Government (Access to Information) (Variation Order) 2006 makes amendments to Section 100(F) of this Act and as mentioned gives additional rights. It specifies the rights of access to documents for Councillors of principal Councils; this is even if those documents are exempt from public access.

Documents are required to be open to inspection by Councillors if they are exempt, if they relate to the financial and business affairs of any particular person, except to the extent that the information relates to terms proposed to or by the authority in the course of contracts or negotiations, or if they are exempt because they reveal that the authority proposes to give a notice under any enactment or to make an order or direction under any enactment.

At common law, members have the right to access information in which they have a "need to know" in order to carry out their role as Councillors.

The amendment to Section 100(F) does not alter the common law rights of members to have access to this information.

Executive Papers

In addition to rights at common law, Councillors have rights under the Local Government (Access to Information Act) 1985.

All members are entitled to documents in the possession and under the control of the executive relating to business to be transacted at a meeting of the executive.

Members have a further right that arises after meetings are held or decisions taken. This right covers the inspection of documents relating to private executive meetings, executive decisions taken by individual members and key decisions taken by officers.

Certain categories of exempt information are excluded from these rights, as is advice provided by a political adviser or assistant.

Standing Orders

These are procedures adopted by councils to govern their meetings and procedures. In most councils, Standing Orders allow Councillor's attendance at a wide range of meetings during the conduct of private business, with a right to speak at the discretion of the Chair of the meeting.

Access by the Overview and Scrutiny Committee

Councils operating executive arrangements are required to have an overview and scrutiny committee to hold the executive to account.

The access to information rules provide extra rights to members of overview and scrutiny committees, who are entitled to copies of certain documents rather than simply having the right to inspect them.

They are entitled to the additional right to have copies of all exempt documents if they are relevant to issues that they are reviewing or which are included in their work programme. The only exception is documents containing advice provided by a political adviser or assistant.

Right to see other documents

Councillors have rights to see the council's accounts and they may also take advantage of more general rights to see all books, deeds, contracts, bills, vouchers and receipts relating to accounts.

Code of Conduct

Councillors are reminded of the Code of Conduct. A new Model Code for Elected Members came in to effect on 3rd May 2007. It applies members of local authorities in England, following their authority's

adoption of the new code. Further guidance from the Standards Board will be given. Of relevance to this note is the following extract: -

In accordance with Statutory Instrument 2007 No 1159 The Local Authorities [Model Code of Conduct] Order 2007 paragraph 4

4. *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;
(iii) the disclosure is made to a third party for the purpose of obtaining professional advice provided that the third party agrees not to disclose the information to any other person; or
(iv) the disclosure is—
(a) reasonable and in the public interest; and
(b) made in good faith and in compliance with the reasonable requirements of the authority; or
(b) prevent another person from gaining access to information to which that person is entitled by law.

Councillors should seek advice before disclosing or withholding information under these provisions of the code.

Useful Website Information

Blackburn with Darwen Council Information Governance Intranet site:

http://cms.intra.blackburn.gov.uk/server.php?show=ConWebDoc.57463

Online Protecting Information Training Course

http://blackburn.thedevelopmentzone.co.uk/

The Information Commissioners Office

http://ico.org.uk/

Specific Guidance issued by the Information Commissioner's Office for Councillor's

http://www.ico.gov.uk/upload/documents/library/freedom_of_information/detailed_specialist_guides/fep109_information_produced_or_received_by_councillors_v1.0.pdf

---

The Department of Constitutional Affairs

http://www.dca.gov.uk/foi/guidance/index.htm

Freedom of Information explained

http://www.freedomofinformation.co.uk/

Local Government Association

http://www.lga.gov.uk/

Model Code of Conduct

http://www.opsi.gov.uk/si/si2007/20071159.htm

This guidance document has been produced by Blackburn with Darwen Council in conjunction with the Association of Greater Manchester Authorities, revised in March 2014.